



Fortisolator - Administration Guide

Version 1.2.1

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://fortiguard.com/>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



August 7, 2019

Fortisolator 1.2.1 Administration Guide

51-121-540944-20190807

TABLE OF CONTENTS

Change log	4
About this release	5
New in this release	5
Overview	6
Fortisolator models	6
Installation	7
Downloading Fortisolator firmware	7
Fortisolator appliance installation	7
Installing Fortisolator 1000F	7
Fortisolator VM installation	16
Installing Fortisolator VM for Linux KVM	16
Installing Fortisolator VM for VMware vSphere	26
Installing Fortisolator VM for VMware ESXi	35
Upgrade	41
Fortisolator appliance upgrade	41
Upgrading Fortisolator firmware using a web browser	41
Upgrading Fortisolator firmware using a USB flash drive	41
Configuration	42
Setting up Fortisolator	42
Configuring the console	42
Port forwarding	46
Getting started in the Fortisolator UI	57
Logging in to the Fortisolator UI	57
Configuring time settings	58
Changing the administrator password	58
Configuring interface settings	58
Configuring DNS settings	59
Configuring routing settings	59
Configuring web filter profiles	61
Configuring security settings	66
Configuring administrator settings	67
Configuring high availability	67
Configuring the login disclaimer	69
Operation	71
Run web browsers through Fortisolator	71
IP forwarding mode	71
Proxy mode	78
PAC file mode	89
Copying and pasting text	99
Diagnostics	100
Diagnostic tools	100

Change log

Date	Change description
2019-08-07	Fortisolator version 1.2.1 document release. See New in this release on page 5 .

About this release

This section provides information about new features in Fortisolator version 1.2.1.

New in this release

Fortisolator version 1.2.1 includes the following new features:

- Virtual serial console connection support on Fortisolator VM for Linux KVM, see [Installing Fortisolator VM for Linux KVM on page 16](#)
- USB flash drive option for Fortisolator firmware upgrades, see [Upgrading Fortisolator firmware using a USB flash drive on page 41](#)
- Fortisolator access through port forwarding, see [Port forwarding on page 46](#)
- Security settings to enable or disable keyboard input and right button on mouse, see [Configuring security settings on page 66](#)
- Fortisolator CLI commands for high availability configuration, see [Configuring high availability on page 67](#)
- Copy and paste options in browsers that run through Fortisolator, see [Copying and pasting text on page 99](#)

Overview

Fortisolator is a browser isolation solution, which protects users against zero day malware and phishing threats that are delivered over the web and email. These threats may result in data loss, compromise, or ransomware. This protection is achieved by creating a visual air gap between users' browsers and websites, which prevents content from breaching the gap. With Fortisolator, web content is executed in a remote disposable container and displayed to users visually, isolating any threat.

For more overview information about Fortisolator, see the [Fortisolator product page](#) and the [Fortisolator data sheet](#).

Fortisolator models

Fortisolator is available in the following appliance and virtual machine models. These models allow you to select the most appropriate solution for your requirements.

- Fortisolator 1000F
- Fortisolator VM for Linux KVM
- Fortisolator VM for VMware vSphere
- Fortisolator VM for VMware ESXi

Fortisolator is available in the following appliance and virtual machine models:

Model	Description
Fortisolator appliance	<ul style="list-style-type: none">• Fortisolator 1000F• Supports 500 concurrent sessions, under normal traffic profiles
Fortisolator VM	<ul style="list-style-type: none">• VMware vSphere Hypervisor ESX/ESXi versions 6.0 and 6.5• KVM QEMU version 0.12.1 and higher, includes a hypervisor

Installation

The following sections provide installation instructions for each model:

- [Installing Fortisolator 1000F](#)
- [Installing Fortisolator VM](#)

Downloading Fortisolator firmware

Use this procedure to download Fortisolator firmware for your Fortisolator model.

Steps

1. Go to <https://support.fortinet.com>.
2. Click **Login** and log in to the Fortinet Support website.
3. From the **Download** menu, select **Firmware Images**.
4. In the **Select Product** drop-down menu, select **Fortisolator**.
5. Select the **Download** tab.
6. In the **Image Folders/Files** section, navigate to the Fortisolator firmware file for your Fortisolator model.
7. To download the firmware, click **HTTPS**.
8. Unzip the firmware file.

For more information about downloading specific firmware versions for your Fortisolator model, see the [Fortisolator Release Notes](#).

Fortisolator appliance installation

Installing Fortisolator 1000F

Use this procedure to install Fortisolator 1000F.

Prerequisites

- Install Fortisolator 1000F hardware, by following the instructions in the [Fortisolator 1000F QuickStart Guide](#).
- Download the Fortisolator firmware, by following the instructions in [Downloading Fortisolator firmware on page 7](#).
- Connect to a console (for example, Tera Term).

Steps

1. Using the console, load the Fortisolator firmware file (for example, FIS_1000F-v1-build0084.out).

```
FortiBootLoader
>FortiIsolator-1000F (10:46-03.28.2018)
>Ver:TST20010
FortiIsolator-1000F (16:27-07.06.2018)
Ver:00020010
Serial number:FISlKFT6l8000001
Total RAM: 131072MB
Boot up, boot device capacity: 1960MB.
Press any key to display configuration menu...
....
[C]: Configure TFTP parameters.
[R]: Review TFTP parameters.
[T]: Initiate TFTP firmware transfer.
[F]: Format boot device.
[B]: Boot with backup firmware and set as default.
[Q]: Quit menu and continue to boot.
[H]: Display this list of options.

Enter C,R,T,F,B,Q,or H:

Image download port:      1
DHCP status:             enabled
Local VLAN ID:           none
Local IP address:        N/A
Local subnet mask:       N/A
Local gateway:           N/A
TFTP server IP address: 172.30.156.3
Firmware file name:      isolator.out

Enter C,R,T,F,B,Q,or H:

Please connect TFTP server to Ethernet port "1".
MAC:          00:90:0B:50:1D:98

Image download port:      1
DHCP status:             enabled
Local VLAN ID:           none
IP:                      172.30.156.159
Subnet:                  255.255.255.0
Gateway:                 172.30.156.254
TFTP server IP address: 172.30.156.3
Firmware file name:      isolator.out
#####
Total 131696234 bytes data downloaded.
Verifying the integrity of the firmware image..

Total 270336kB unzipped.
```

```
Image download port: 1
DHCP status: enabled
Local VLAN ID: none
IP: 172.30.156.159
Subnet: 255.255.255.0
Gateway: 172.30.156.254
TFTP server IP address: 172.30.156.3
Firmware file name: isolator.out
#####
Total 131696234 bytes data downloaded.
Verifying the integrity of the firmware image..

Total 270336kB unzipped.

Save as Default firmware/Backup firmware/Run image without saving:[D/B/R]?d
Programming the boot device now.
.....
Reading boot image 7084460 bytes.
INIT: version 2.88 booting...
INIT: Entering runlevel: 3
Starting logging: OK
ext2fs_check_if_mount: Can't check if filesystem is mounted due to missing mtab
/dev/sda: recovering journal
/dev/sda: clean, 1364/61054976 files, 4348813/244190646 blocks
Image version: 1.2.0.0065
Isolator version: 1.2.0.0061
renaming eth0 to internal
renaming eth1 to external
renaming eth4 to mgmt
Populating /dev using udev: done
Initializing random number generator... done.
Starting system message bus: done
Starting network: OK
ip: RTNETLINK answers: File exists
ip: RTNETLINK answers: File exists
ip: RTNETLINK answers: File exists
Starting dropbear sshd: OK
Starting crond: OK
Starting httpd: OK
Starting ha: OK
Now starting webfilter ...
Starting startx: OK

Welcome to Isolator
FISlKFT6l8000001 login: █
```

2. Boot in to the Fortisolator login. The default username is **admin** and there is no default password.

```

Welcome to Isolator
FIS1KFT618000001 login: admin
Password:
> show
Configured parameters:
      Interface  internal  IPv4 IP:    192.168.1.100/24  MAC: 00:90:0B:50:1D:98
      Interface  external IPv4 IP:    172.30.157.1/24  MAC: 00:90:0B:50:1D:99
      Interface  mgmt     IPv4 IP:    172.30.156.46/24  MAC: 00:90:0B:6D:A3:3B
IPv4 Internal Gateway: :                192.168.1.254
IPv4 External Gateway: :                172.30.157.254
IPv4 MGMT Gateway:    :                172.30.156.254
hostname              :                FIS1KFT618000001
dns server            :                172.16.100.100
dns server            :                172.16.100.80
build number          :                0065(interim)
date time             :                2019-05-02 13:05:25 PDT
> status
System Status:
Version           :                v1.2.0-build0065 (Interim)
Serial number     :                FIS1KFT618000001
System time       :                Thu May 02 13:05:27 2019 PDT
Disk Usage        :                1014360 bytes
Disk Size         :                960381672 bytes
Max Sessions      :                2048
Active Sessions   :                0
>

```

3. Configure the network parameters (first time only). For example:

Configured parameters:

```

Interface  internal  IPv4 IP:    192.168.1.100/24
Interface  external IPv4 IP:    172.30.157.1/24
Interface  mgmt     IPv4 IP:    172.30.156.46/24
IPv4 Internal Gateway:    192.168.1.254
IPv4 External Gateway:    172.30.157.254

hostname    :                FIS1KFT618000001
dns server  :                172.16.100.100
dns server  :                172.16.100.80
build number:                0065(interim)
date time   :                2019-05-02 13:05:25 PDT

```

4. Set the time zone.

```
> show
Configured parameters:
      Interface  internal  IPv4 IP:    192.168.1.100/24  MAC: 00:90:0B:50:1D:98
      Interface  external IPv4 IP:    172.30.157.1/24  MAC: 00:90:0B:50:1D:99
      Interface      mgmt   IPv4 IP:    172.30.156.46/24  MAC: 00:90:0B:6D:A3:3B
IPv4 Internal Gateway: :                192.168.1.254
IPv4 External Gateway: :                172.30.157.254
IPv4 MGMT Gateway:    :                172.30.156.254
hostname              :                FIS1KFT618000001
dns server            :                172.16.100.100
dns server            :                172.16.100.80
build number         :                0065(interim)
date time             :                2019-05-02 13:05:25 PDT
```

5. You can use the `show` command to see the settings (for example, IP addresses, gateway address, DNS server information, and build number).

```
> show
Configured parameters:
      Interface  internal  IPv4 IP:    192.168.1.100/24  MAC: 00:90:0B:50:1D:98
      Interface  external IPv4 IP:    172.30.157.1/24  MAC: 00:90:0B:50:1D:99
      Interface      mgmt   IPv4 IP:    172.30.156.46/24  MAC: 00:90:0B:6D:A3:3B
IPv4 Internal Gateway: :                192.168.1.254
IPv4 External Gateway: :                172.30.157.254
IPv4 MGMT Gateway:    :                172.30.156.254
hostname              :                FIS1KFT618000001
dns server            :                172.16.100.100
dns server            :                172.16.100.80
build number         :                0065(interim)
date time             :                2019-05-02 13:05:25 PDT
```

6. You can use the `status` command to see system information (for example, build version, serial number, system time, disk usage, disk size, and sessions information).

```
> status
System Status:
Version          :                v1.2.0-build0065 (Interim)
Serial number    :                FIS1KFT618000001
System time      :                Thu May 02 13:05:27 2019 PDT
Disk Usage       :                1014360 bytes
Disk Size        :                960381672 bytes
Max Sessions     :                2048
Active Sessions  :                0
>
```

7. You can use the `help` command to see the Fortisolator console comments.

```
COM1 - Tera Term VT
File Edit Setup Control Window Help
>
> help
Fortisolator Console
General:
  help      Display this text
  ?         Synonym for 'help'
  exit      Exit from the CLI
Configuration:
  show      Show bootstrap configuration
           Available attributes/values for show:
           ha-all          <null>
           ha-enabled      0/1
           ha-group-id     [1-255]
           ha-lost-threshold [1-60]
           ha-interval      [1-20]
                           in unit of 100ms
           ha-hello-holddown [5-300]
                           in unit of seconds
           ha-priority      [0-255]
                           255 means not used
           ha-allow-override 0/1
           ha-schedule      <schedule type>
           ha-virtual-ip    <IP/netmask>
                           e.g. 192.168.100.2/24
           ha-password      <PASSWORD>
           ha-password-enc  <Encoded PASSWORD>
           ha-interface     <Interface Name>
                           e.g. internal/external/mgmt

  show-ipmap-ha  Show HA ipmapping configuration
  set           Set configuration parameter
           Available attributes/values for set:
           internal-ip      <IP/netmask>
                           e.g. 192.168.100.2/24
           external-ip      <IP/netmask>
                           e.g. 192.168.100.2/24
           mgmt-ip          <IP/netmask>
                           e.g. 192.168.100.2/24
           date             <YYYY-MM-DD>
           time             <HH:MM:SS>
           dns              <pdns-ip sdns-ip>
                           e.g. 192.168.100.1 192.168.10.1
           ntp              <ntp-ip>
                           e.g. 192.168.100.1
           internal-gw       <SUBNET> <Gateway IP>
                           e.g. 192.168.100.0/24 192.168.100.1
           external-gw       <SUBNET> <Gateway IP>
                           e.g. 192.168.100.0/24 192.168.100.1
           mgmt-gw           <SUBNET> <Gateway IP>
                           e.g. 192.168.100.0/24 192.168.100.1
           hostname         <hostname>
           timezone         <timezone>
                           e.g. America/Los_Angeles
           ha-enabled      0/1
           ha-group-id     [1-255]
           ha-lost-threshold [1-60]
           ha-interval      [1-20]
                           in unit of 100ms
           ha-hello-holddown [5-300]
                           in unit of seconds
           ha-priority      [0-255]
                           255 means not used
           ha-allow-override 0/1
           ha-schedule      <schedule type>
           ha-virtual-ip    <IP/netmask>
                           e.g. 192.168.100.2/24
           ha-password      <PASSWORD>
           ha-password-enc  <Encoded PASSWORD>
           ha-interface     <Interface Name>
                           e.g. internal/external/mgmt
           fis-ipmap-ha      <priority external_isolator_ip internal_isolator_ip external_po
rt internal_port>
                           e.g. 0 192.168.100.1 10.1.0.1 12443 12887
           fis-ipmap        <external_port internal_port [external_isolator_ip]>
                           e.g. 12443 12887 192.168.100.1
           fis-ipmap-vip    <external_port internal_port external_isolator_ip>
                           e.g. 14443 14887 192.168.122.1

  unset      Unset configuration parameter
           Available attributes for unset:
           dns
           ntp
           internal-gw
           external-gw
           mgmt-gw
           fis-ipmap-ha
           fis-ipmap
```

```

COM1 - Tera Term VT
File Edit Setup Control Window Help

ha-priority          [0-255]
                     255 means not used
ha-allow-override    0/1
ha-schedule           <schedule type>
ha-virtual-ip         <IP/netmask>
                     e.g. 192.168.100.2/24
ha-password          <PASSWORD>
ha-password-enc       <Encoded PASSWORD>
ha-interface          <Interface Name >
                     e.g. internal/external/mgmt

show-ipmap-ha        Show HA ipmapping configuration
set                  Set configuration parameter
                     Available attributes/values for set:

                     internal-ip      <IP/netmask>
                                     e.g. 192.168.100.2/24
                     external-ip     <IP/netmask>
                                     e.g. 192.168.100.2/24
                     mgmt-ip         <IP/netmask>
                                     e.g. 192.168.100.2/24
                     date            <YYYY-MM-DD>
                     time            <HH:MM:SS>
                     dns             <pdns-ip sdns-ip>
                                     e.g. 192.168.100.1 192.168.10.1
                     ntp             <ntp-ip>
                                     e.g. 192.168.100.1
                     internal-gw     <SUBNET> <Gateway IP>
                                     e.g. 192.168.100.0/24 192.168.100.1
                     external-gw     <SUBNET> <Gateway IP>
                                     e.g. 192.168.100.0/24 192.168.100.1
                     mgmt-gw         <SUBNET> <Gateway IP>
                                     e.g. 192.168.100.0/24 192.168.100.1
                     hostname        <hostname>
                     timezone        <timezone>
                                     e.g. America/Los_Angeles
                     ha-enabled      0/1
                     ha-group-id     [1-255]
                     ha-lost-threshold [1-60]
                     ha-interval     [1-20]
                                     in unit of 100ms
                     ha-hello-holddown [5-300]
                                     in unit of seconds
                     ha-priority     [0-255]
                                     255 means not used
                     ha-allow-override 0/1
                     ha-schedule     <schedule type>
                     ha-virtual-ip   <IP/netmask>
                                     e.g. 192.168.100.2/24
                     ha-password     <PASSWORD>
                     ha-password-enc <Encoded PASSWORD>
                     ha-interface    <Interface Name >
                                     e.g. internal/external/mgmt
                     fis-ipmap-ha     <priority external_isolator_ip internal_isolator_ip external_po
rt internal_port>
                                     e.g. 0 192.168.100.1 10.1.0.1 12443 12887
                     fis-ipmap       <external_port internal_port [external_isolator_ip]>
                                     e.g. 12443 12887 192.168.100.1
                     fis-ipmap-vip    <external_port internal_port external_isolator_ip>
                                     e.g. 14443 14887 192.168.122.1

unset                Unset configuration parameter
                     Available attributes for unset:

                     dns
                     ntp
                     internal-gw
                     external-gw
                     mgmt-gw
                     fis-ipmap-ha
                     fis-ipmap
                     fis-ipmap-vip

System:
  reboot             Reboot the Fortiisolator
  system-upgrade     Upgrade Fortiisolator System Image
  factory-reset       Reset configuration to defaults and delete all data
  shutdown           Shutdown the Fortiisolator
  status             Display some status information
  admin-pwd-reset     Reset Admin Password

Utilities:
  nslookup           Basic tool for DNS debugging
  ping               Test network connectivity to another network host
  fnsysctl disp       Display conf, category or log
  fnsysctl tail       Display the last part of conf, category or log

Diagnostics:
  hardware-info       Display general hardware status information
  diagnose-nic        Display general network interface setting
  diagnose-wf         Test and show WF action for an URL

```

Fortisolator VM installation

To install Fortisolator VM, follow the procedure for one of the following VM systems:

- [Installing Fortisolator VM for Linux KVM on page 16](#)
- [Installing Fortisolator VM for VMware vSphere on page 26](#)
- [Installing Fortisolator VM for VMware ESXi on page 35](#)

Installing Fortisolator VM for Linux KVM

Use this procedure to install Fortisolator VM for Linux KVM.

Fortisolator VM for Linux KVM supports both Video Graphics Array (VGA) and virtual serial console connections.

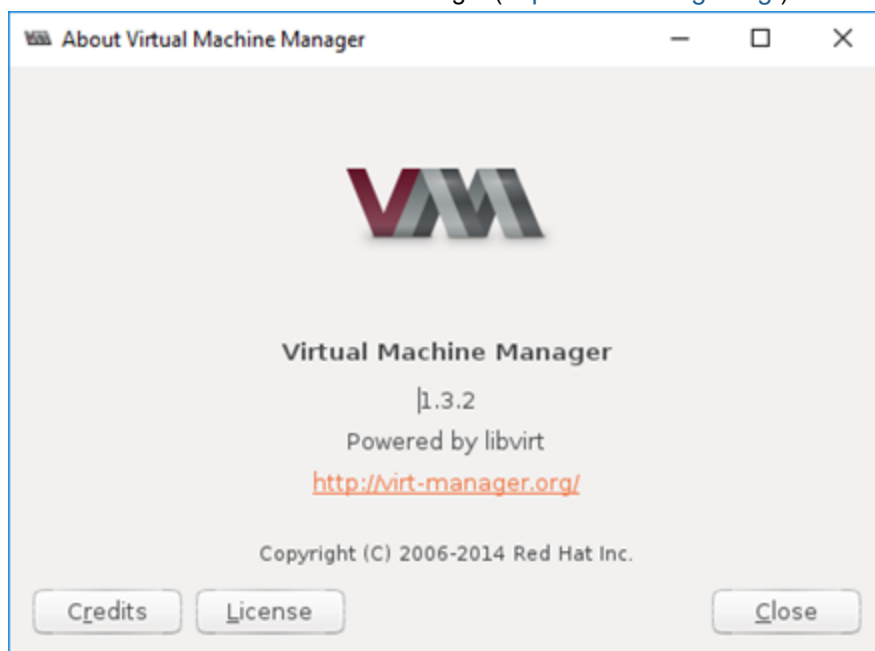
Prerequisites

- Ensure that your system has at least two hard disks of the following types:
 - IDE
 - SATA
 - SCSI
 - Virtio
- Ensure that your system has at least three network interfaces of the following types:
 - Hypervisor default (Rt18139)
 - E1000

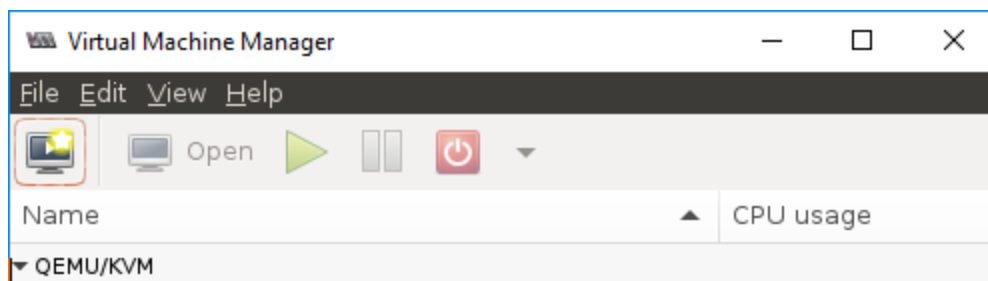
Steps

1. Download the Fortisolator firmware for KVM by following the instructions in [Downloading Fortisolator firmware on page 7](#).

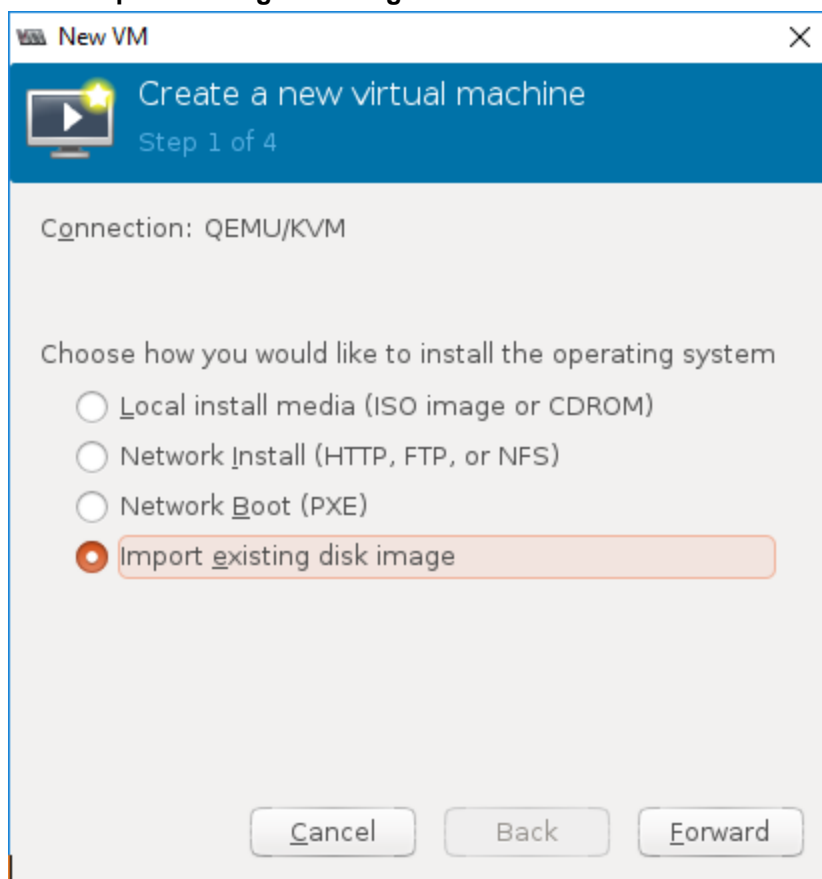
2. Launch KVM with Virtual Machine Manager (<https://virt-manager.org/>).



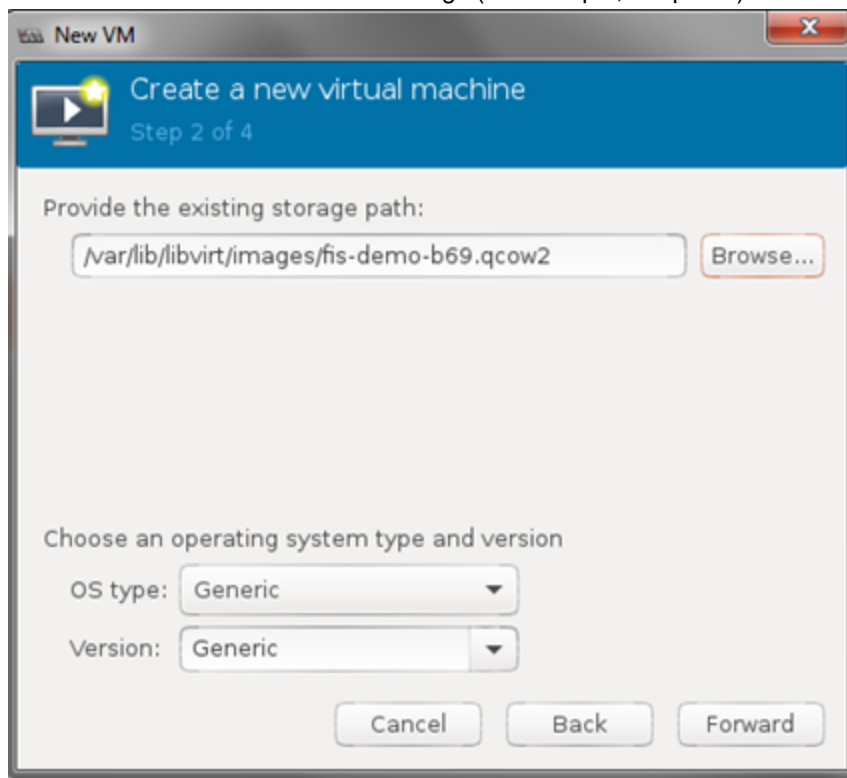
3. Create a new virtual machine.



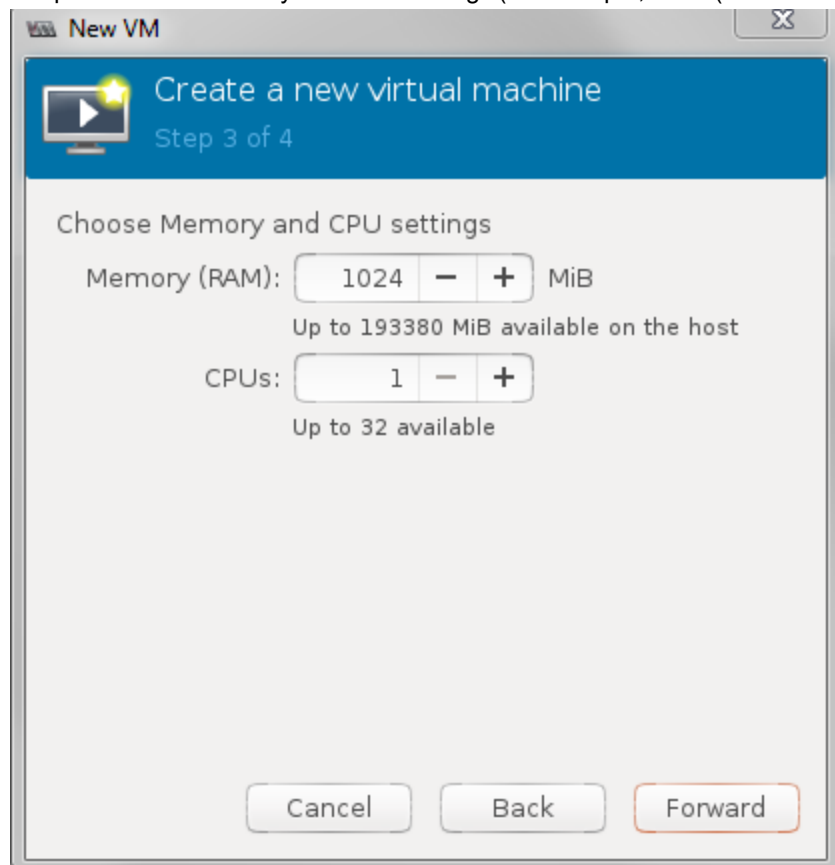
4. Select **Import existing disk image**.



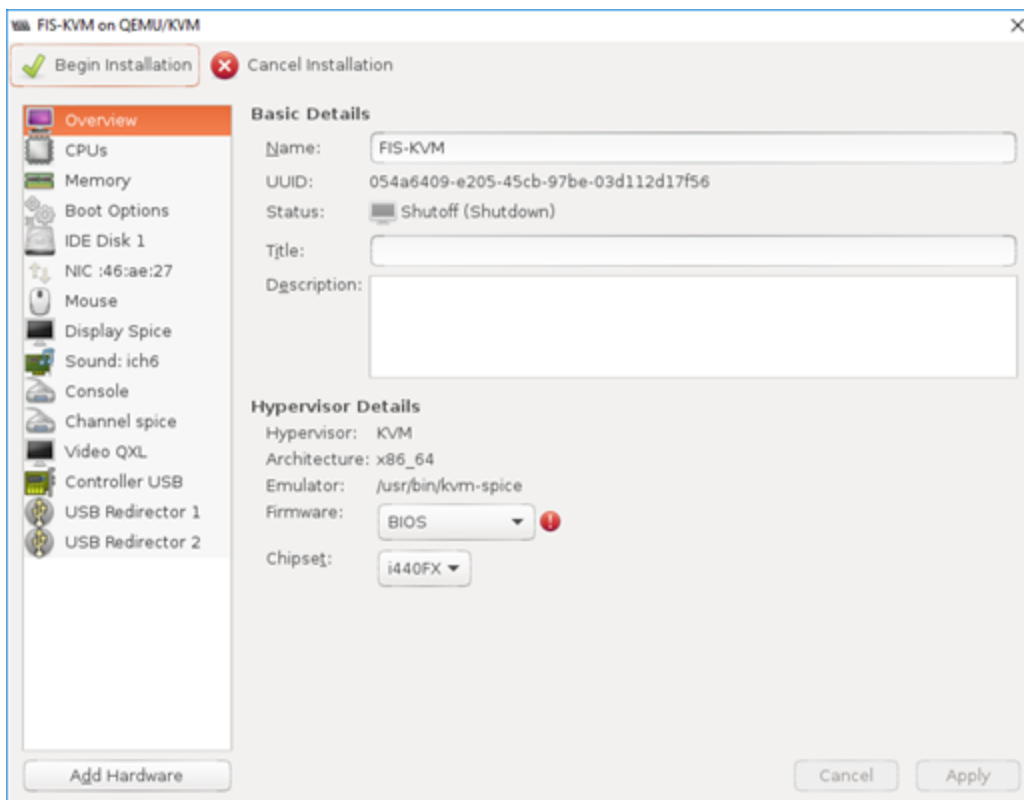
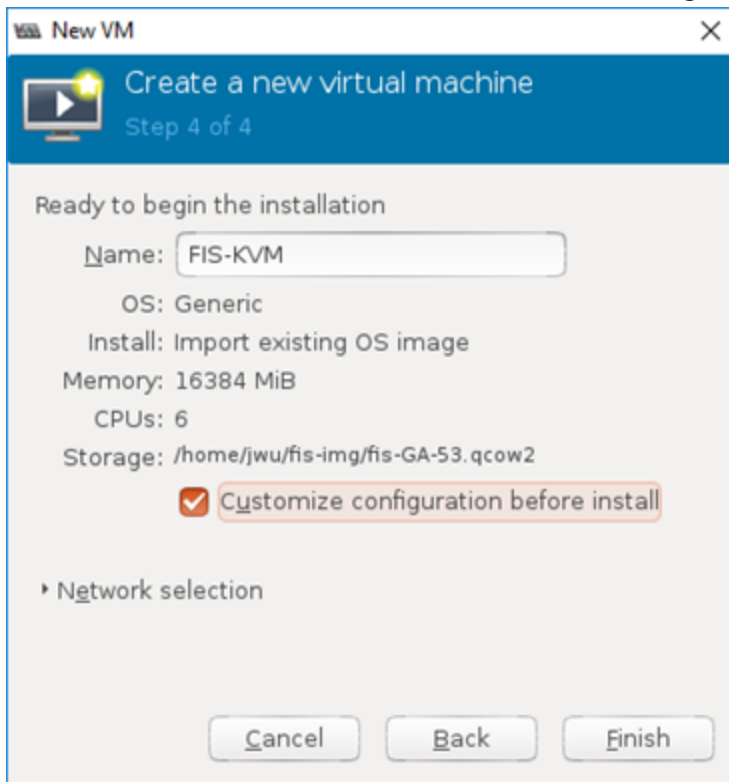
5. Browse and select the Fortisolator image (for example, fis.qcow2).



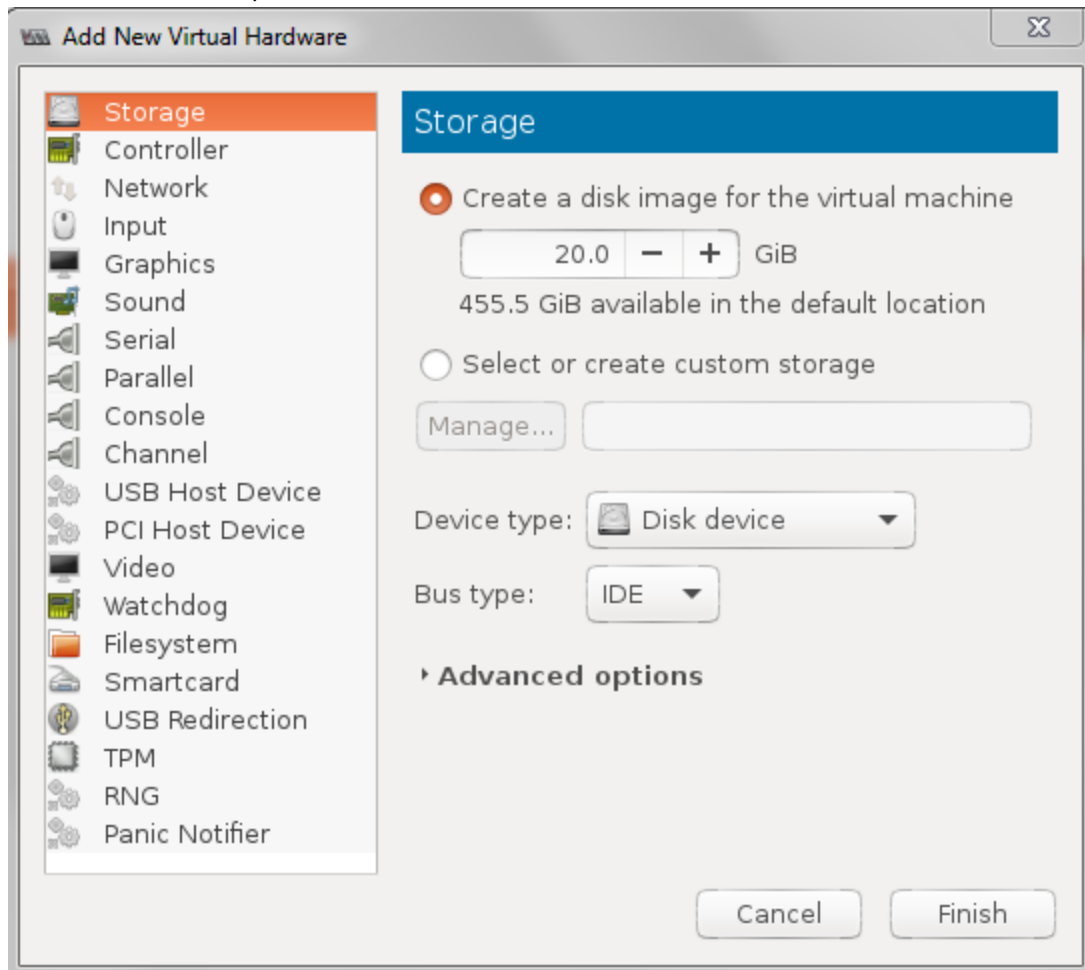
6. Keep the default memory and CPU settings (for example, 1024 (193380 MiB) of memory and 1 CPU).



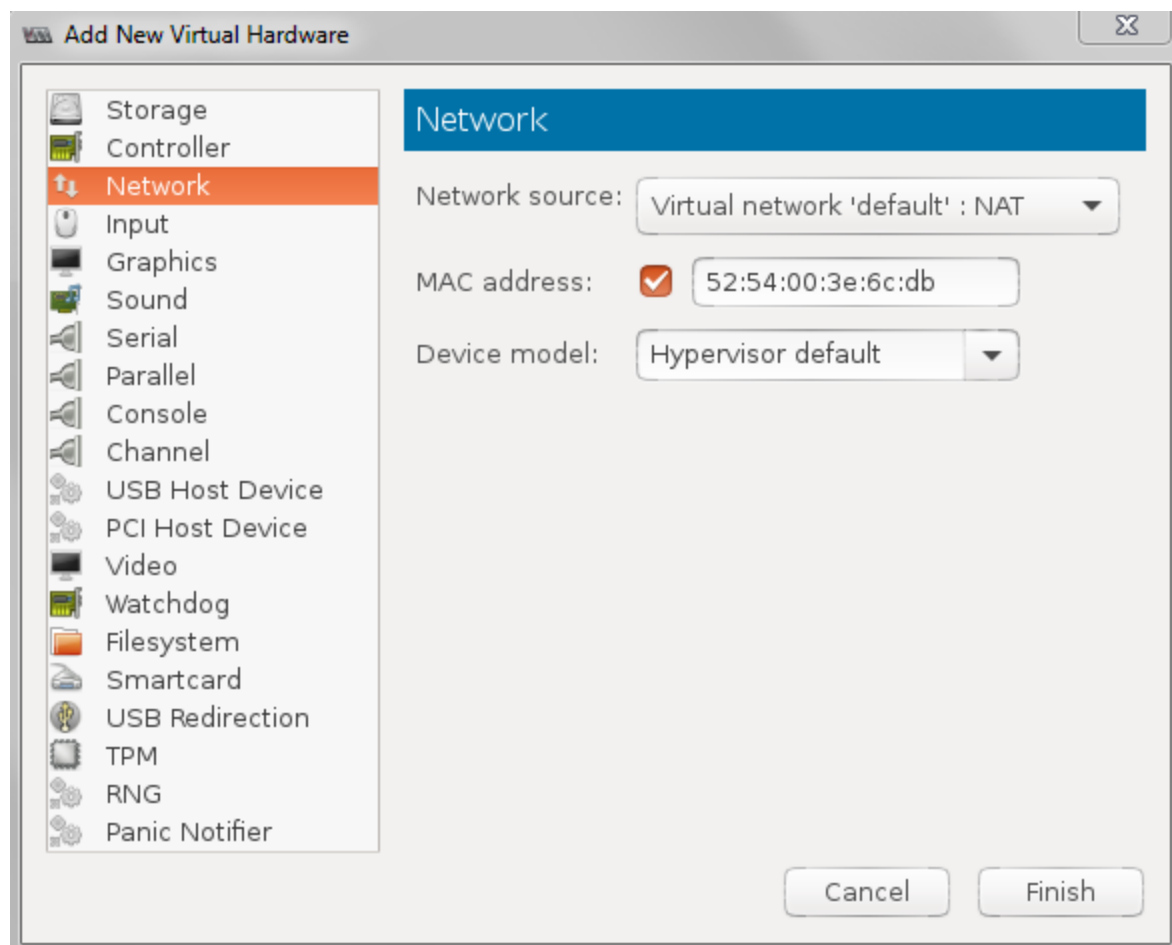
7. Name the new virtual machine, and select **Customize configuration before install**.



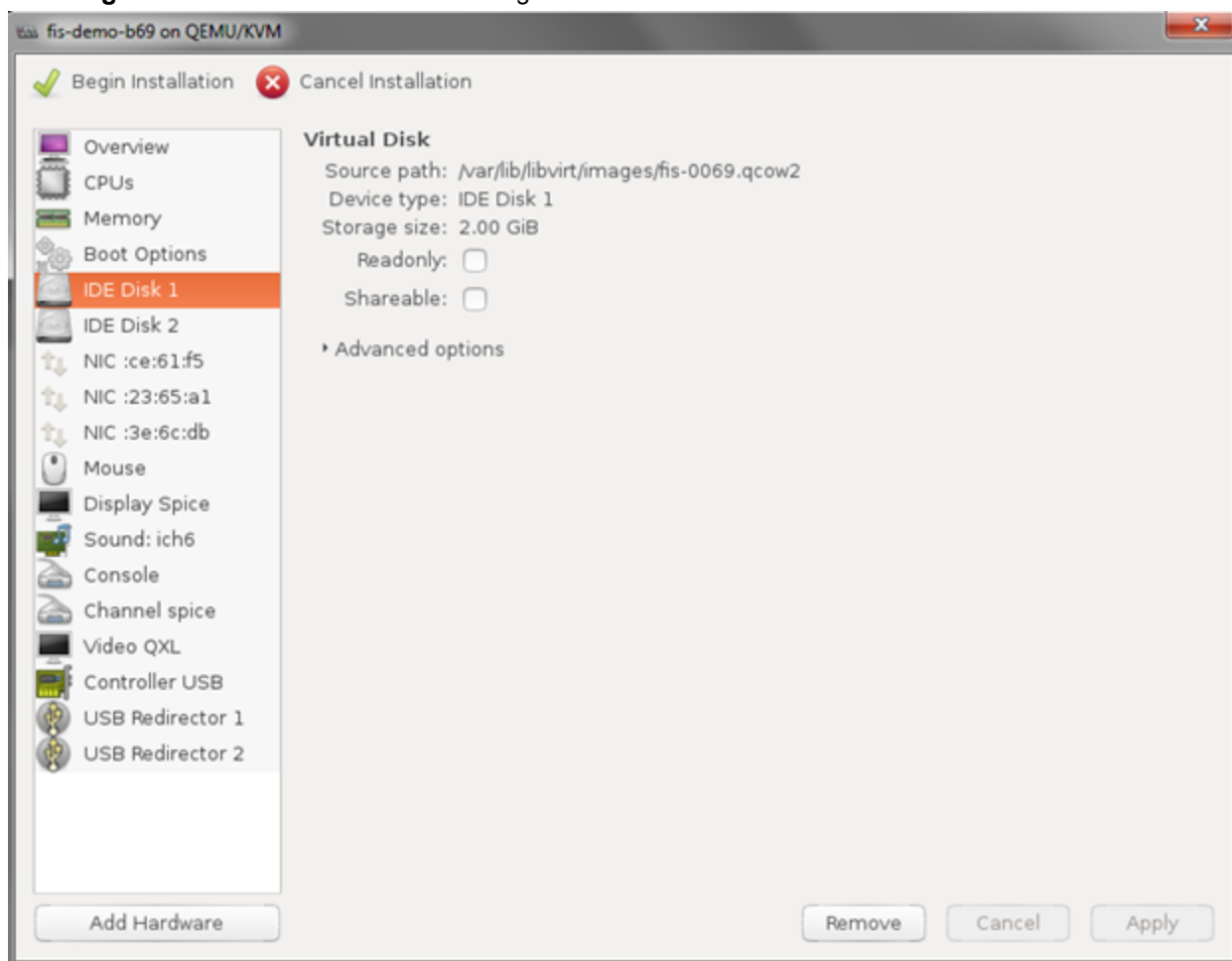
8. Add an IDE disk. Accept the default values.

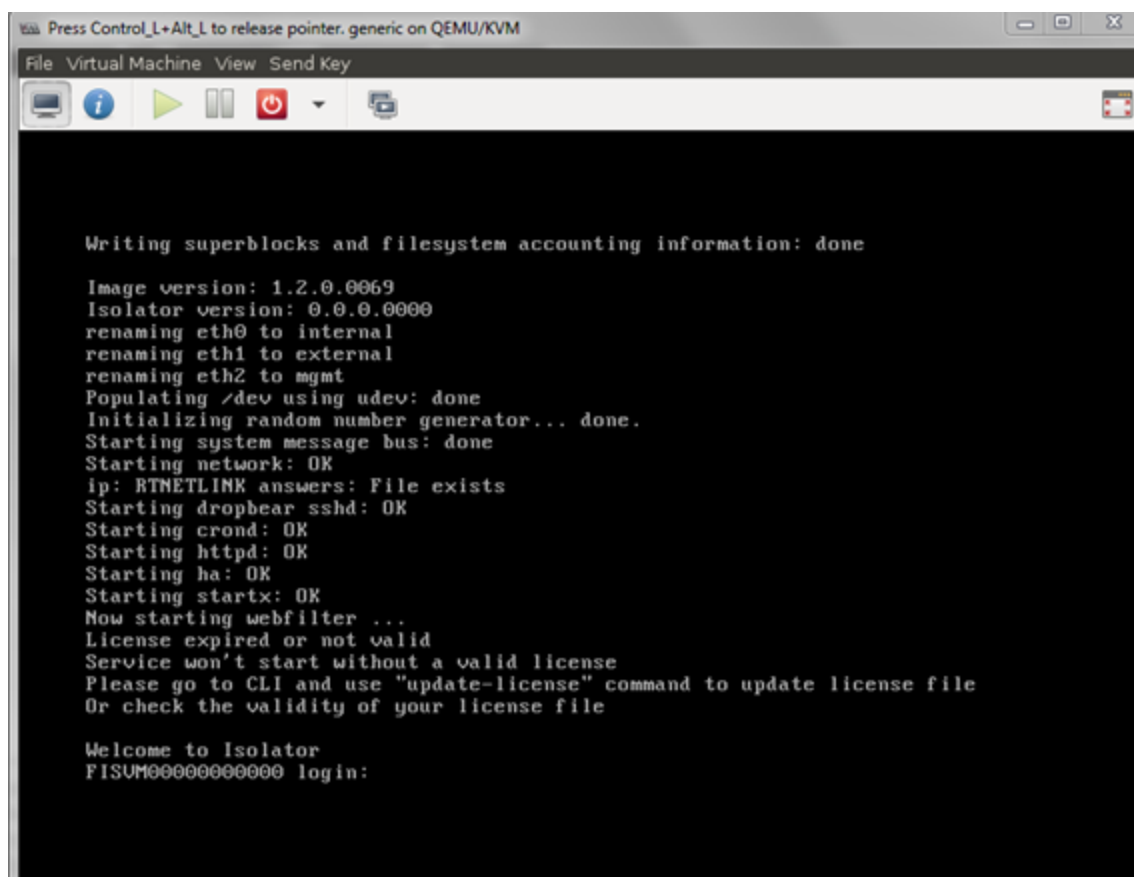
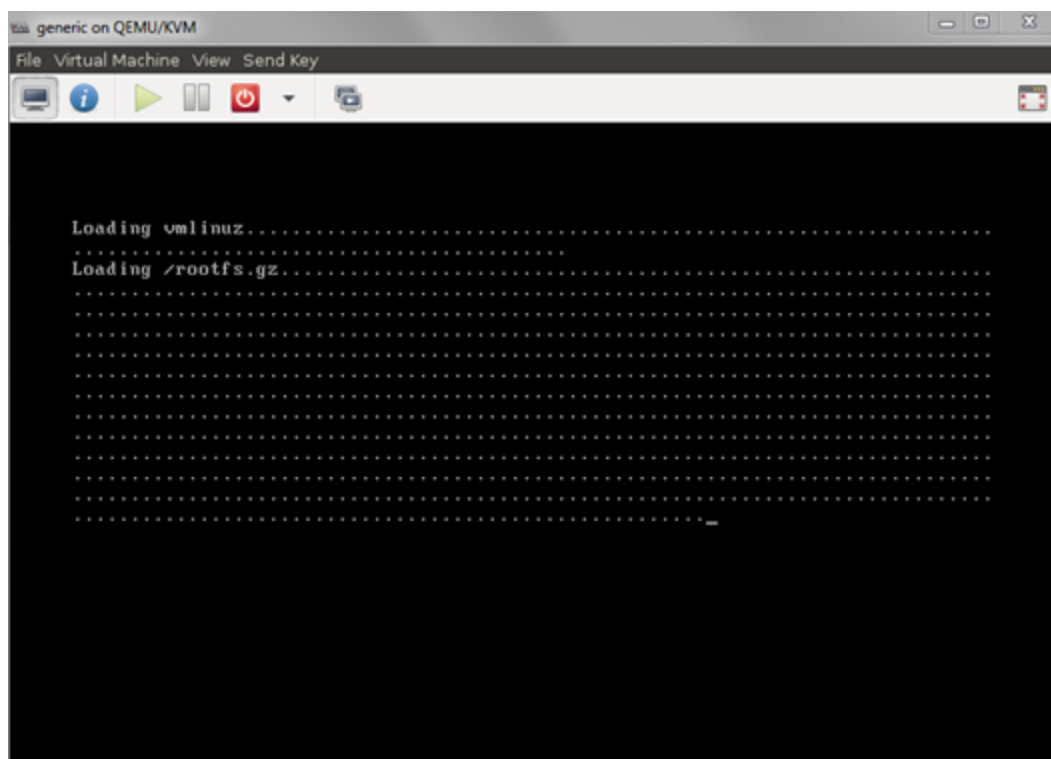


9. Add two network interfaces: one for Network 2 and one for Network 3. Leave the settings for **Network source** (Virtual network 'default':NAT) and **Device model** (Hypervisor default) at their default values.



10. Click **Begin Installation** to load the KVM image.





11. In the **Set default parameters** step, configure the network interfaces.

```
set internal-ip      192.168.122.99/24
set internal-gw      192.168.122.0/24      192.168.122.254
set external-ip      172.30.156.99/24
set external-gw      0.0.0.0/0            172.30.156.254
set mgmt-ip          192.168.199.99/24
set mgmt-gw          192.168.199.0/24      192.168.199.254
set dns              208.91.112.53 208.91.112.52
```

Installing Fortisolator VM for VMware vSphere

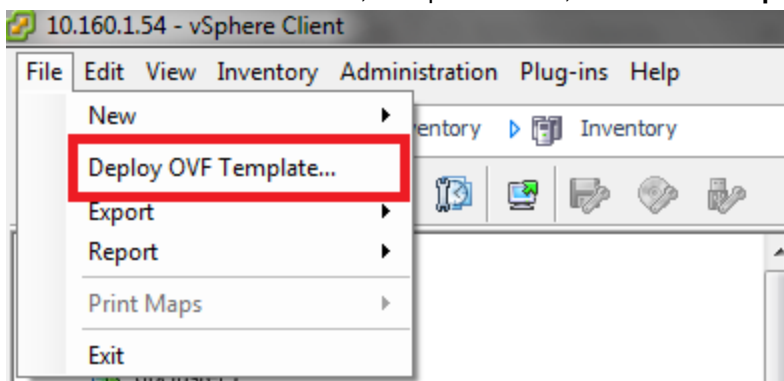
Use this procedure to install Fortisolator VM for VMware vSphere.

Prerequisites

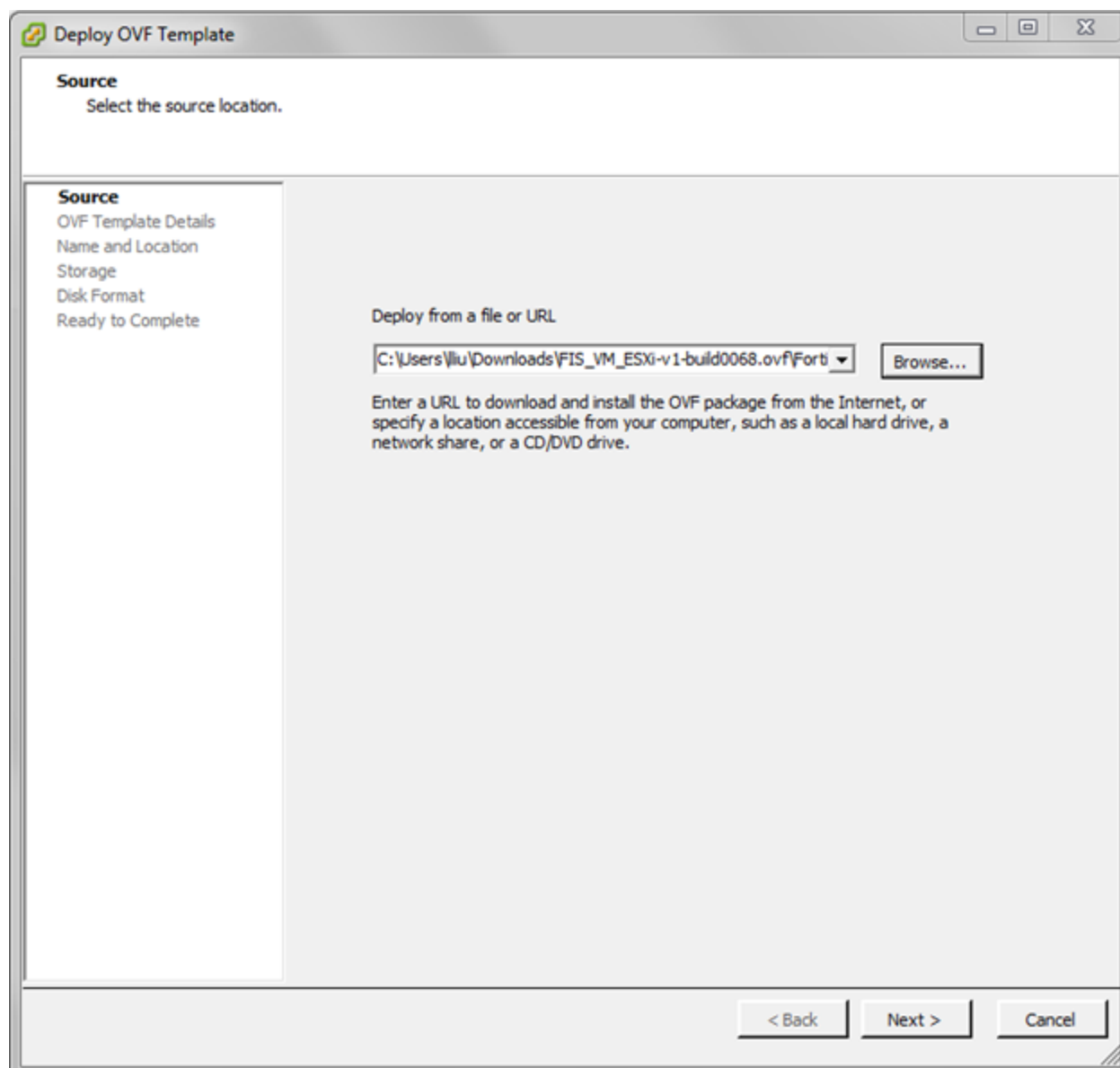
- Install VMware vSphere Client.
- Ensure that your system has one of the following combinations of hard disks and network adapters to support ESXi 6.0:
 - Two SCSI hard disks and three VMXNET 3 network adapters (this is the default)
 - One IDE hard disk and one SCSI hard disk and three E1000 network adapters

Steps

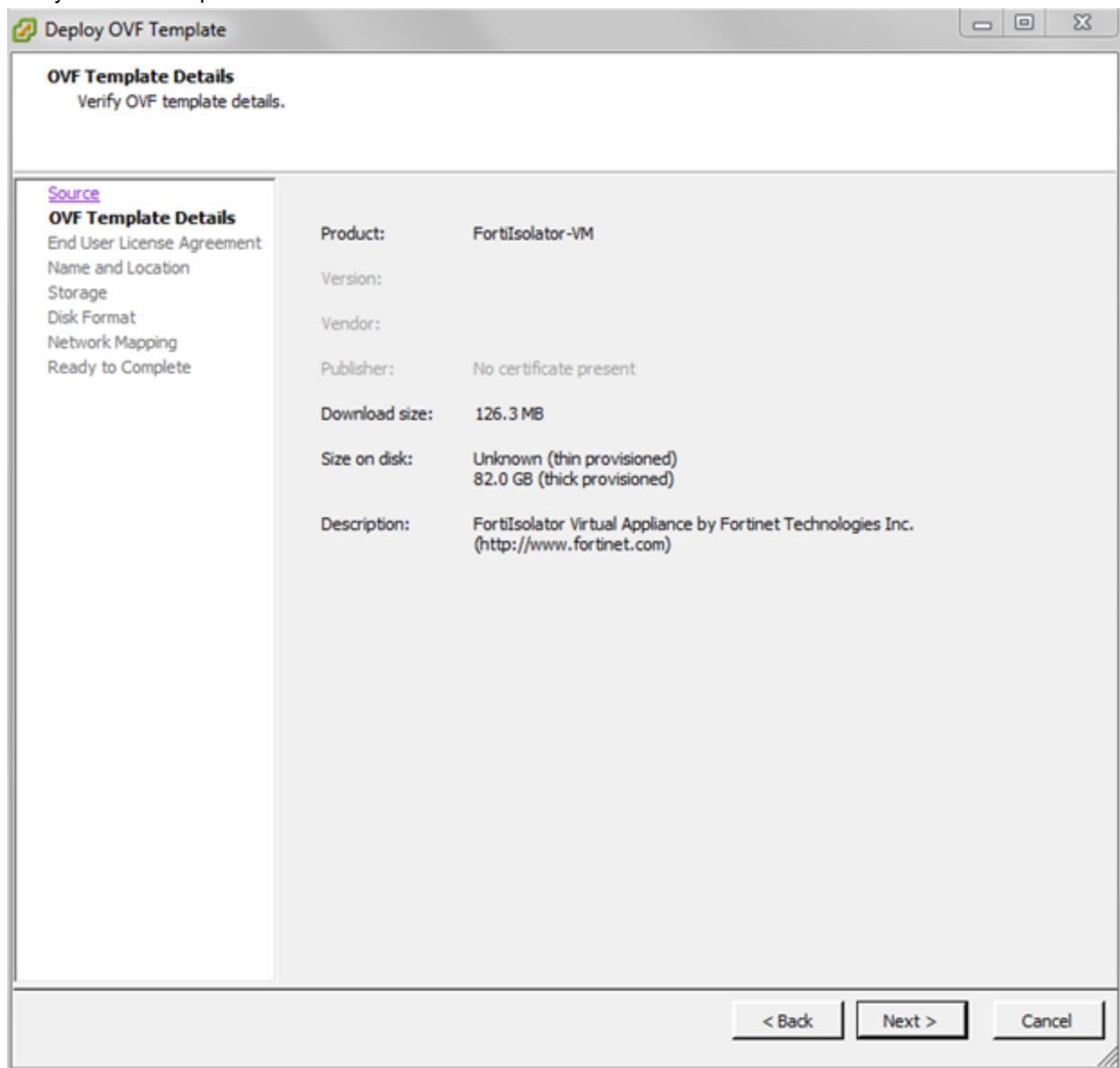
1. Download the Fortisolator firmware for VMware by following the instructions in [Downloading Fortisolator firmware on page 7](#).
2. To create a new virtual machine, in vSphere Client, select **File > Deploy OVF Template**.



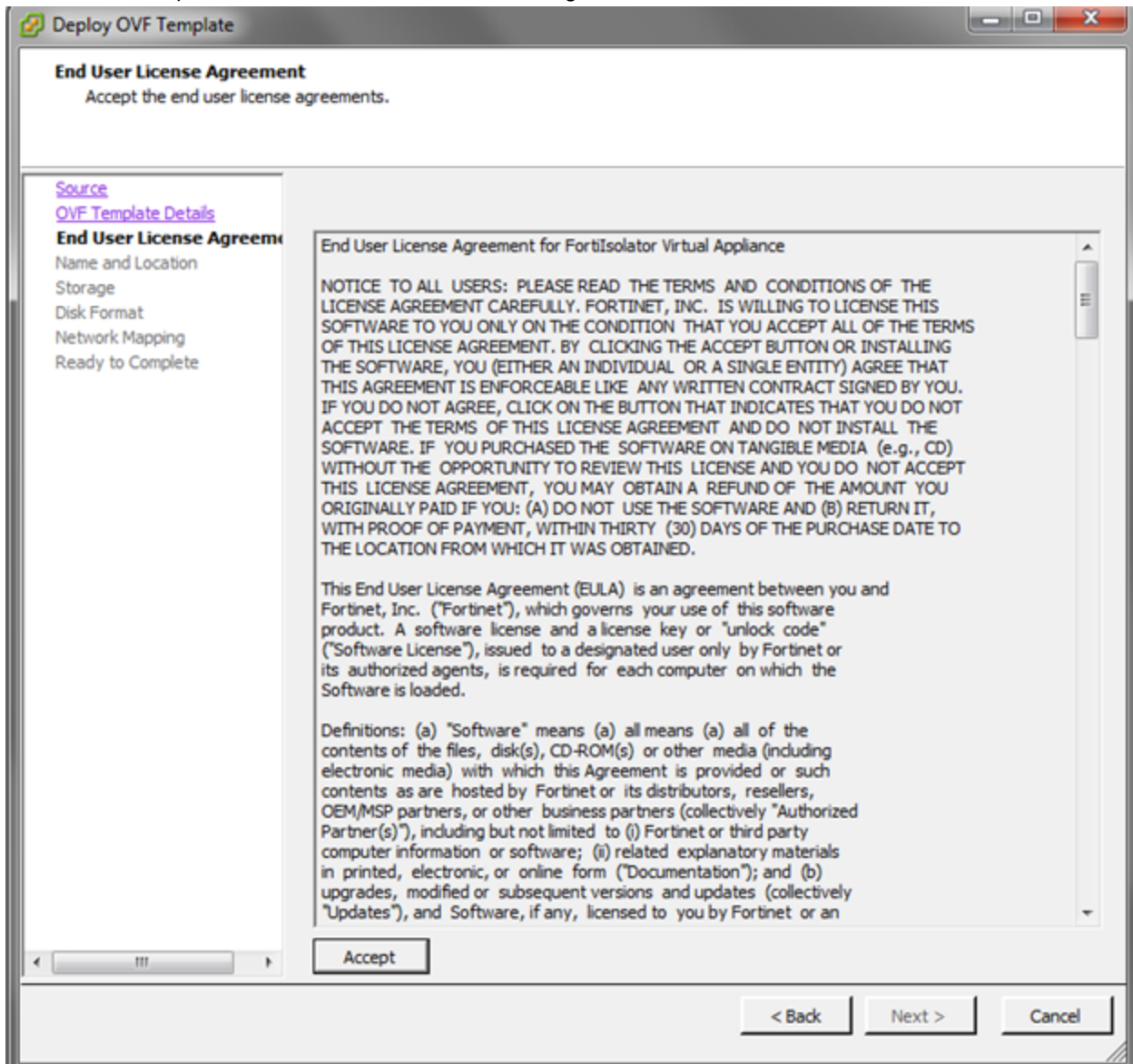
3. Browse to the folder that contains the Fortisolator files and select **Fortisolator.ovf**.



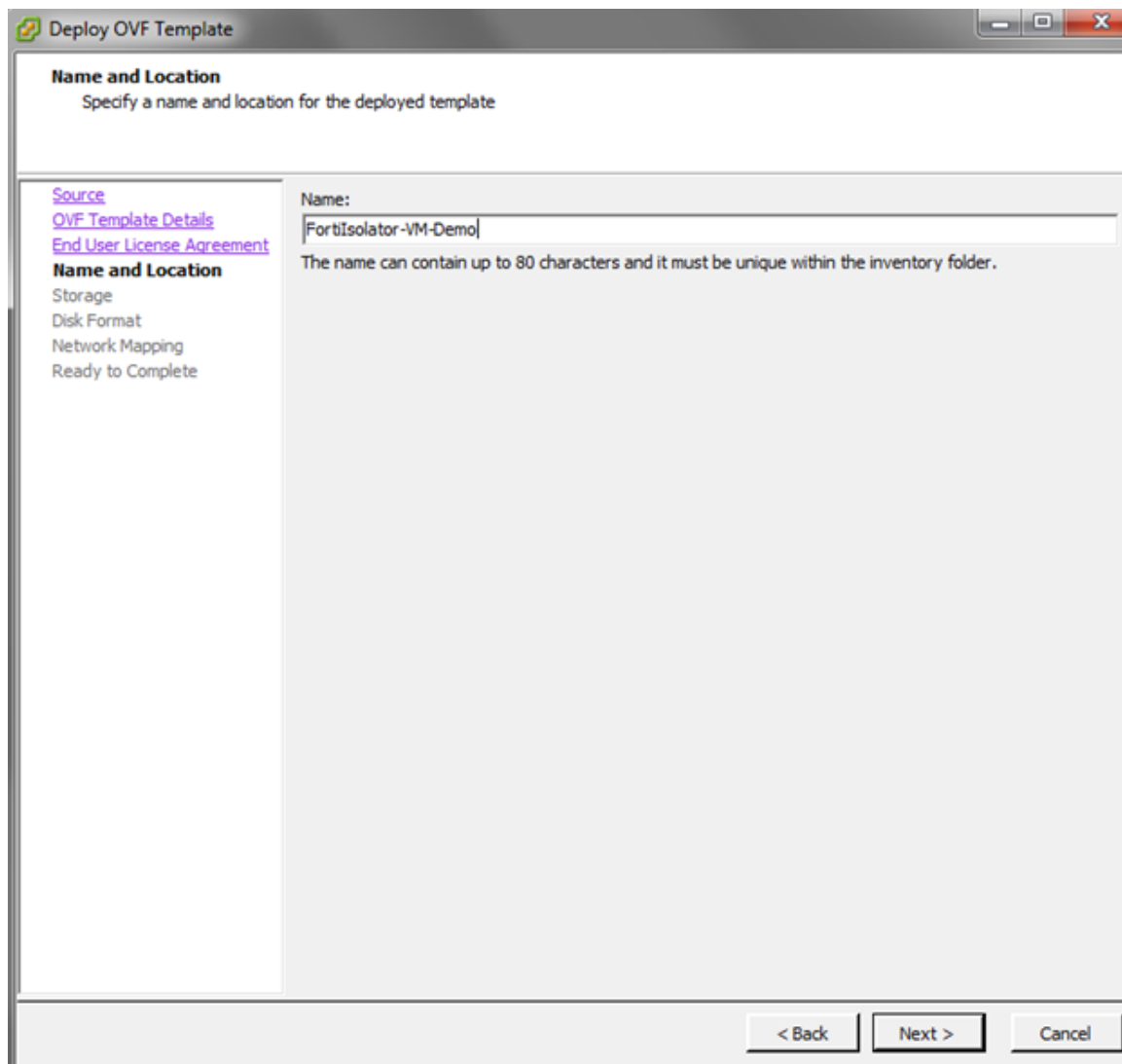
4. Verify the OVF template details.



5. Review and accept the Fortisolator End User License Agreement.



6. Name the new Fortisolator virtual machine.



The screenshot shows the 'Deploy OVF Template' wizard window. The title bar reads 'Deploy OVF Template'. The main heading is 'Name and Location' with the instruction 'Specify a name and location for the deployed template'. On the left, a sidebar lists the steps: 'Source', 'OVF Template Details', 'End User License Agreement', 'Name and Location' (which is highlighted), 'Storage', 'Disk Format', 'Network Mapping', and 'Ready to Complete'. The main area has a 'Name:' label followed by a text input field containing 'Fortisolator-VM-Demo'. Below the input field, a note states: 'The name can contain up to 80 characters and it must be unique within the inventory folder.' At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Deploy OVF Template

Name and Location
Specify a name and location for the deployed template

[Source](#)
[OVF Template Details](#)
[End User License Agreement](#)
Name and Location
Storage
Disk Format
Network Mapping
Ready to Complete

Name:
Fortisolator-VM-Demo

The name can contain up to 80 characters and it must be unique within the inventory folder.

< Back Next > Cancel

7. Select the datastore where you want to install the Fortisolator VM.

Storage
Where do you want to store the virtual machine files?

[Source](#)
[OVF Template Details](#)
[End User License Agreement](#)
[Name and Location](#)
Storage
Disk Format
Network Mapping
Ready to Complete

Select a destination storage for the virtual machine files:

Name	Drive Type	Capacity	Provisioned	Free	Type	Thin Provi
datastore1	Non-SSD	411.00 GB	572.43 GB	56.84 GB	VMFSS	Supporte
Main-Disk	Non-SSD	2.73 TB	6.98 TB	15.52 GB	VMFSS	Supporte

☐ Disable Storage DRS for this virtual machine

Select a datastore:

Name	Drive Type	Capacity	Provisioned	Free	Type	Thin Provi
------	------------	----------	-------------	------	------	------------

Compatibility:
Insufficient disk space for full capacity of 82.00 GB. Thin provisioned disk size is unknown.

< Back Next > Cancel

8. Select the disk provisioning format. For optimal performance, select a **Thick Provision** option.

The screenshot shows the 'Deploy OVF Template' window with the 'Disk Format' step selected. The window title is 'Deploy OVF Template'. The main heading is 'Disk Format' with the subtext 'In which format do you want to store the virtual disks?'. On the left, a sidebar lists navigation options: 'Source', 'OVF Template Details', 'End User License Agreement', 'Name and Location', 'Storage', 'Disk Format' (highlighted), 'Network Mapping', and 'Ready to Complete'. The main area displays 'Datastore:' with a dropdown menu showing 'Main-Disk' and 'Available space (GB):' with a text box showing '15.5'. Below these, three radio button options are listed: 'Thick Provision Lazy Zeroed' (selected), 'Thick Provision Eager Zeroed', and 'Thin Provision'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

9. Configure the required network interfaces. Adding more than three interfaces may result in inconsistent mapping.

Deploy OVF Template

Network Mapping
What networks should the deployed template use?

[Source](#)
[OVF Template Details](#)
[End User License Agreement](#)
[Name and Location](#)
[Storage](#)
[Disk Format](#)
Network Mapping
Ready to Complete

Map the networks used in this OVF template to networks in your inventory

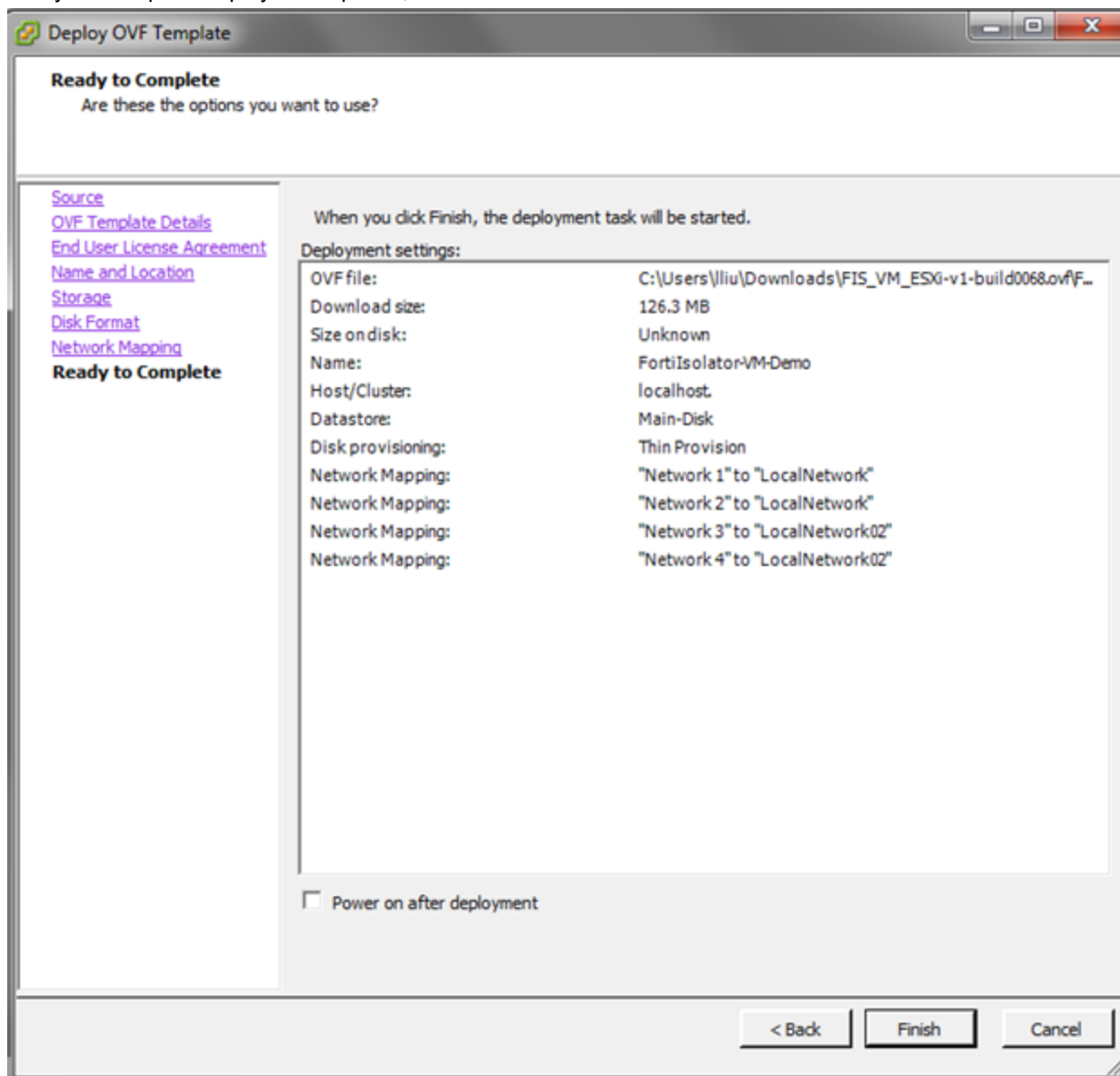
Source Networks	Destination Networks
Network 1	LocalNetwork
Network 2	LocalNetwork
Network 3	LocalNetwork02
Network 4	LocalNetwork02

Description:
The Network 1 network

Warning: Multiple source networks are mapped to the host network: LocalNetwork

< Back Next > Cancel

10. Verify the template deployment options, and click **Finish**.



11. Start the Fortisolator VM.

```
Writing superblocks and filesystem accounting information: done

Image version: 1.2.0.0050
Isolator version: 0.0.0.0000
renaming eth0 to internal
renaming eth1 to external
renaming eth2 to mgmt
Populating /dev using udev: done
Initializing random number generator... done.
Starting system message bus: done
Starting network: OK
ip: RTNETLINK answers: File exists
Starting dropbear sshd: OK
Starting crond: OK
Starting httpd: OK
Starting ha: OK
Starting startx: OK
Now starting webfilter ...
License expired or not valid
Service won't start without a valid license
Please go to CLI and use "update-license" command to update license file
Or check the validity of your license file

Welcome to Isolator
FISUM0000000000 login: _
```

12. Log in to Fortisolator. The default username is **admin** and there is no default password.

Installing Fortisolator VM for VMware ESXi

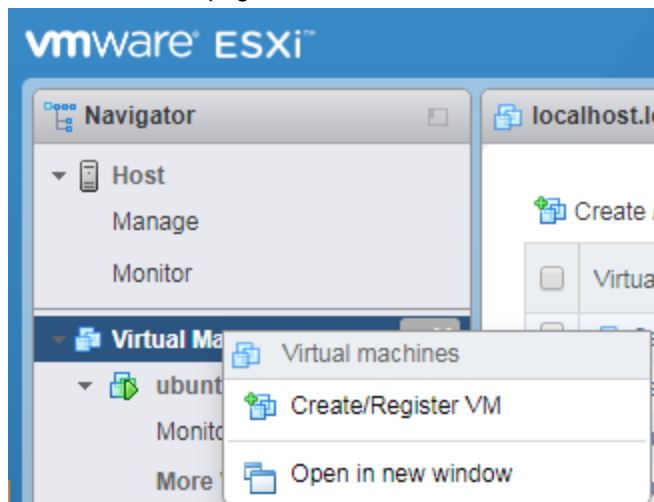
Use this procedure to install Fortisolator VM for VMware ESXi.

Prerequisites

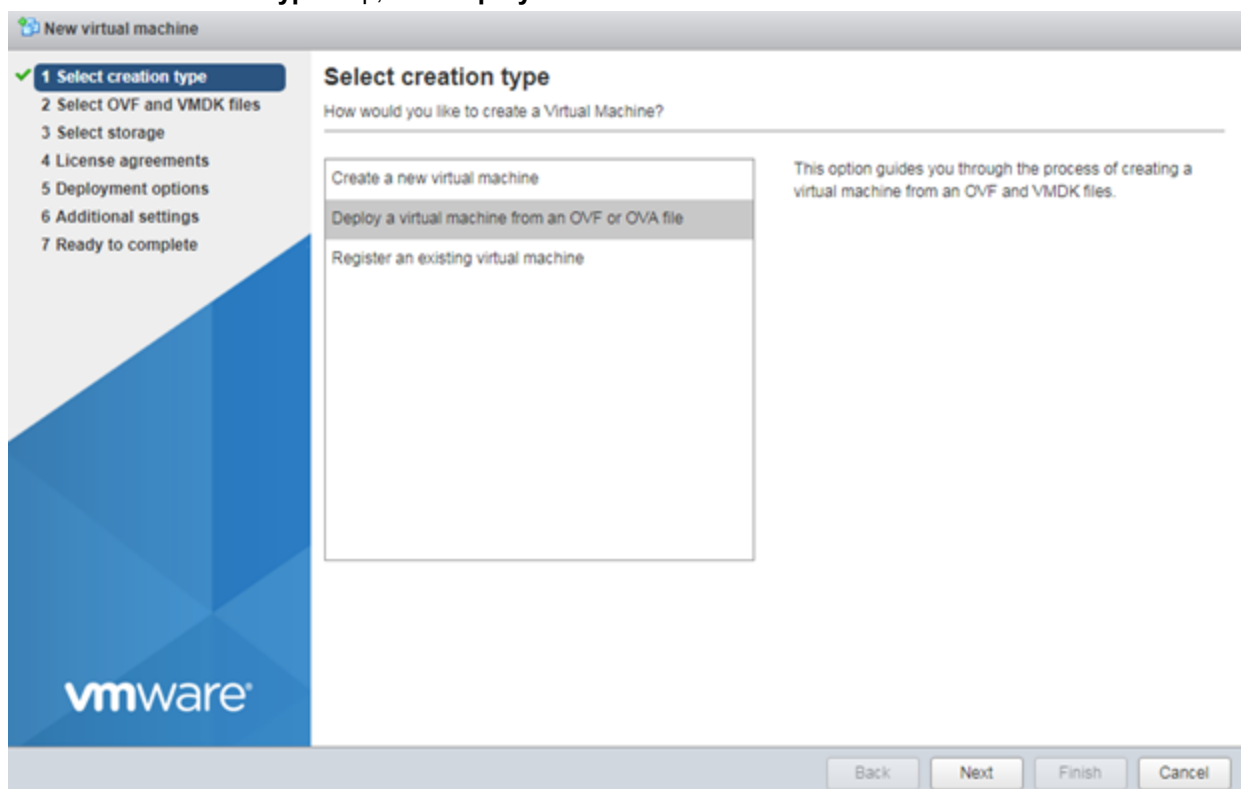
- Install VMware vSphere Client.
- Ensure that your system has one of the following combinations of hard disks and network adapters to support ESXi 6.5:
 - Two SCSI hard disks and three VMXNET 3 network adapters (this is the default)
 - Two SCSI hard disks and three E1000 network adapters

Steps

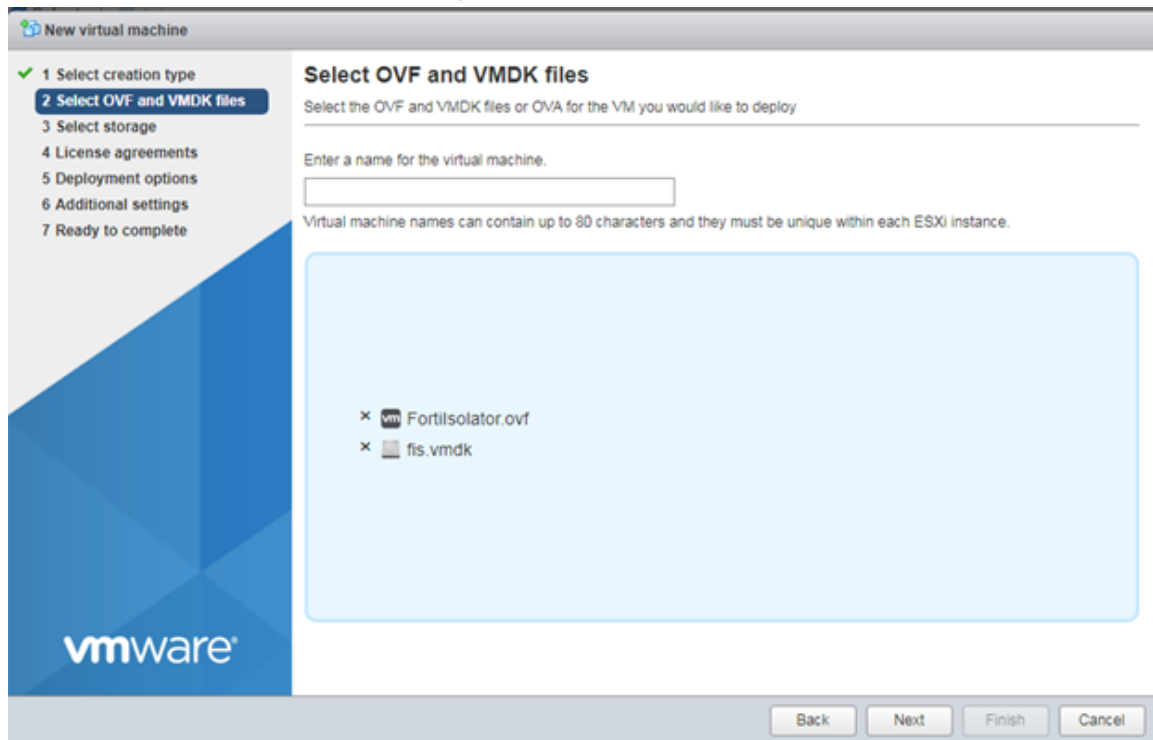
1. In the ESXi home page, click **Virtual Machine**, and then right-click and select **Create/Register VM**.



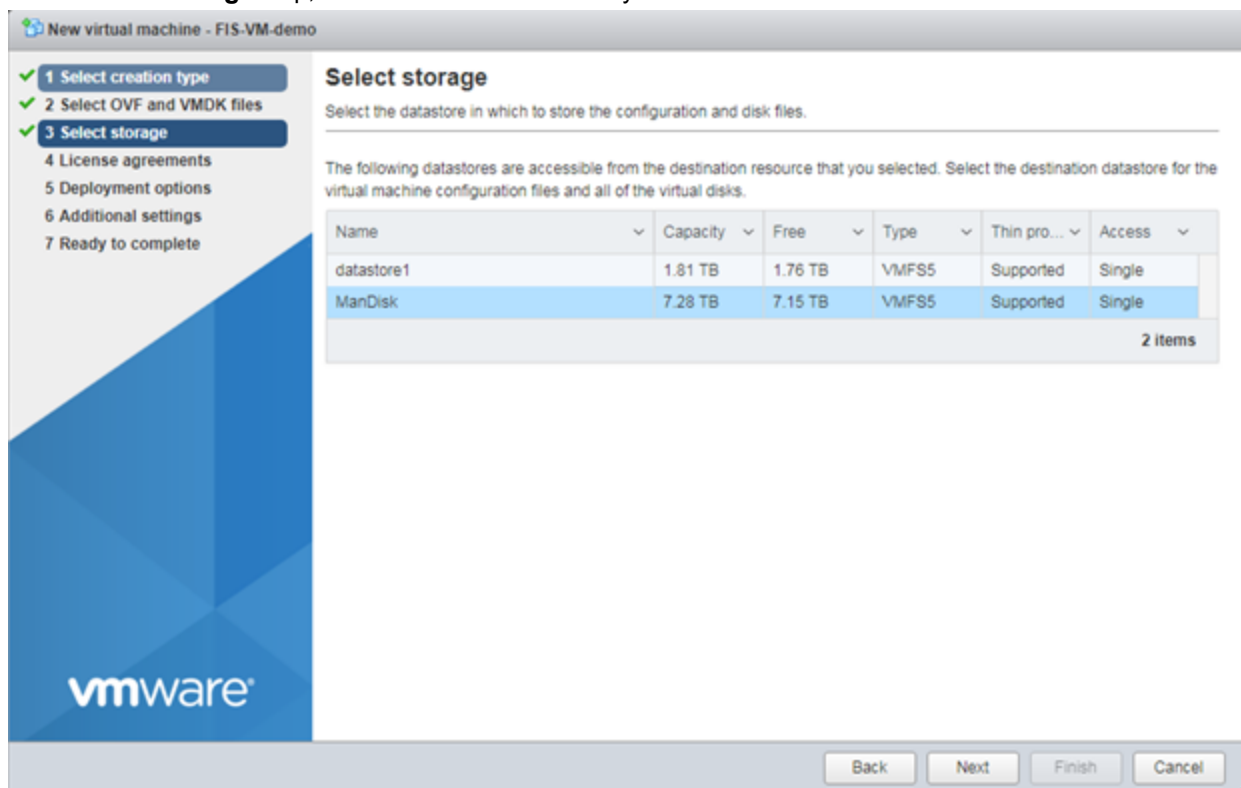
2. In the **Select creation type** step, click **Deploy a virtual machine from an OVF or OVA file**.



3. In the **Select OVF and VMDK files** step, select both the **Fortisolator.ovf** and **fis.vmdk** files.



4. In the **Select storage** step, select the datastore where you want to install the Fortisolator VM.



5. Review and accept the Fortisolator End User License Agreement.

New virtual machine - FIS-VM-demo

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- 4 License agreements**
- 5 Deployment options
- 6 Ready to complete

License agreements

Read and accept the license agreements

An end-user license...

End User License Agreement for FortiIsolator Virtual Appliance

NOTICE TO ALL USERS: PLEASE READ THE TERMS AND CONDITIONS OF THE LICENSE AGREEMENT CAREFULLY. FORTINET, INC. IS WILLING TO LICENSE THIS SOFTWARE TO YOU ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. BY CLICKING THE ACCEPT BUTTON OR INSTALLING THE SOFTWARE, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN CONTRACT SIGNED BY YOU. IF YOU DO NOT AGREE, CLICK ON THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS LICENSE AGREEMENT AND DO NOT INSTALL THE SOFTWARE. IF YOU PURCHASED THE SOFTWARE ON TANGIBLE MEDIA (e.g., CD) WITHOUT THE OPPORTUNITY TO REVIEW THIS LICENSE AND YOU DO NOT ACCEPT THIS LICENSE AGREEMENT, YOU MAY OBTAIN A REFUND OF THE AMOUNT YOU ORIGINALLY PAID IF YOU: (A) DO NOT USE THE SOFTWARE AND (B) RETURN IT, WITH PROOF OF PAYMENT, WITHIN THIRTY (30) DAYS OF THE PURCHASE DATE TO THE LOCATION FROM WHICH IT WAS OBTAINED.

This End User License Agreement (EULA) is an agreement between you and Fortinet, Inc. ("Fortinet"), which governs your use of this software product. A software license and a license key or "unlock code" ("Software License"), issued to a designated user only by Fortinet or its authorized agents, is provided for each computer on which the

I agree

Back Next Finish Cancel

6. In the **Deployment options** step, configure **Network mappings**, **Disk provisioning**, and select the **Power on automatically** checkbox.

New virtual machine - FIS-VM-demo

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- ✓ 4 License agreements
- 5 Deployment options**
- 6 Ready to complete

Deployment options

Select deployment options

Network mappings	Network 1	VM Network ▼
	Network 2	VM Network ▼
	Network 3	VM Network ▼
	Network 4	VM Network ▼

Disk provisioning

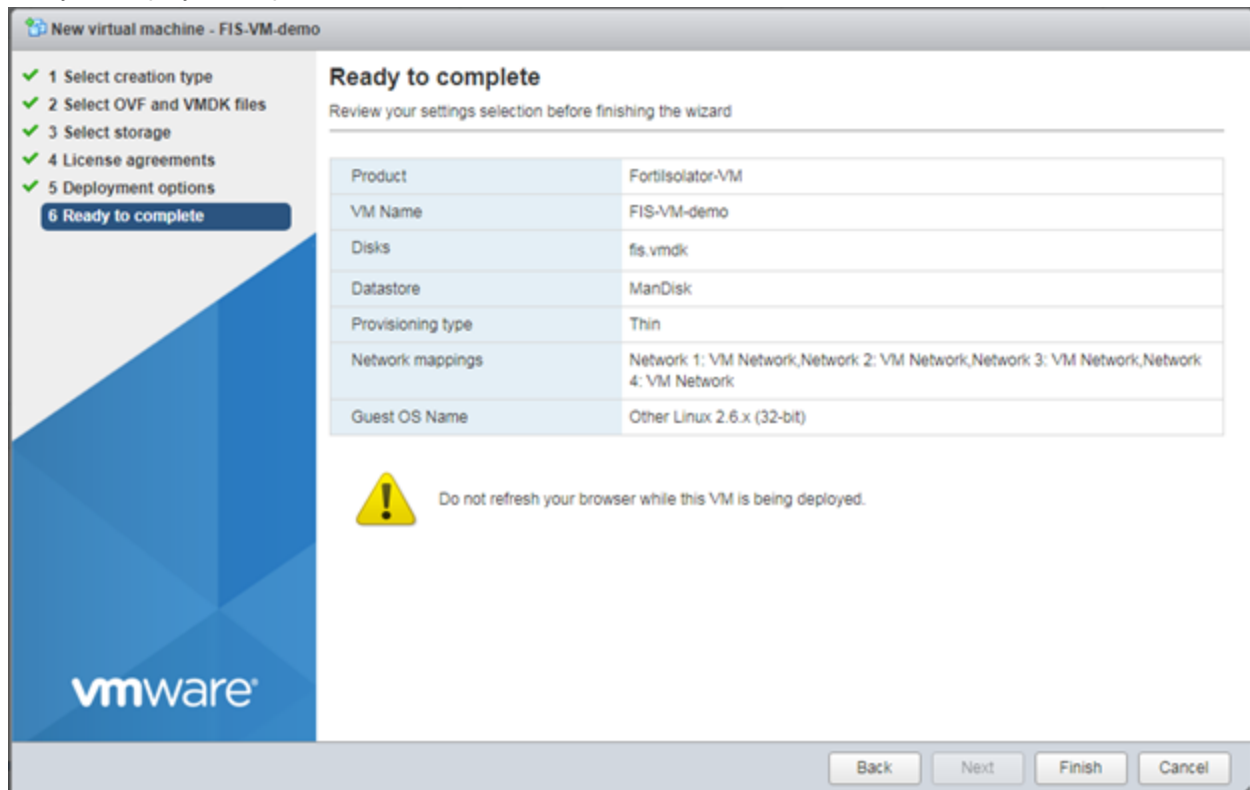
☒ Thin ☐ Thick

Power on automatically

☒

Back Next Finish Cancel

7. Verify the deployment options, and click **Finish**.



8. To start the VM, right-click the Fortisolator VM name, and select **Power > Power on**.
9. To open the Fortisolator VM console, click **Console > Open browser console**.

```

Writing superblocks and filesystem accounting information: done
Image version: 1.2.0.0067
Isolator version: 0.0.0.0000
renaming eth0 to internal
renaming eth1 to external
renaming eth2 to mgmt
Populating /dev using udev: done
Initializing random number generator... done.
Starting system message bus: done
Starting network: OK
ip: RTNETLINK answers: File exists
Starting dropbear sshd: OK
Starting crond: OK
Starting httpd: OK
Starting ha: OK
Now starting webfilter ...
Starting startx: OK
License expired or not valid
Service won't start without a valid license
Please go to CLI and use "update-license" command to update license file
Or check the validity of your license file
Welcome to Isolator
FISUMAAAAAAAAAAAA login:

```

10. Log in to Fortisolator. The default username is **admin** and there is no default password.

11. Configure the IP and gateway addresses for the internal and management interfaces.

```

FIS-VM-demo
killall: isolator: no process killed
kill Xvfb
7.
invalid pattern of mgmt gateway ip:10.160.17.
>
> set mgmt-gw 10.160.17.0/24 10.160.17.1
> Starting startx: OK
License expired or not valid
Service won't start without a valid license
Please go to CLI and use "update-license" command to update license file
Or check the validity of your license file

> show
Configured parameters:
Interface    internal    IPv4 IP:    10.160.16.63/24    MAC: 00:0C:29:B7
:CB:29
Interface    mgmt       IPv4 IP:    10.160.17.63/24    MAC: 00:0C:29:B7
:CB:3D
IPv4 Internal Gateway: :    10.160.16.1
IPv4 MGMT Gateway: :    10.160.17.1
hostname      :    FISUM000000000000
dns server    :    127.0.0.1
build number   :    0067(interim)
date time     :    2019-05-03 18:52:04 UTC
>

```

12. To verify that the internet connection works, ping 8.8.8.8.
13. To access the Fortisolator web portal, use the management IP address (for example, <http://10.160.17.63>).

Upgrade

Fortisolator appliance upgrade

Upgrading Fortisolator firmware using a web browser

Use this procedure to upgrade a Fortisolator hardware appliance, such as the Fortisolator 1000F, using a web browser. You can use the Fortisolator UI or Fortisolator CLI to perform the upgrade.

Fortisolator UI

To perform an upgrade, go to **System > Upgrade**. In the **Upgrade by Web** section, click **Choose File**, and follow the instructions.

Fortisolator CLI

To perform an upgrade, use the `system-upgrade` command.

Upgrading Fortisolator firmware using a USB flash drive

Use this procedure to upgrade a Fortisolator hardware appliance, such as the Fortisolator 1000F, using a USB flash drive. You can use the Fortisolator UI or Fortisolator CLI to perform the upgrade.

Fortisolator UI

To perform an upgrade, go to **System > Upgrade**. In the **Upgrade by USB** section, select **Click here**, and follow the instructions.

Fortisolator CLI

To perform an upgrade, use the `system-upgrade` command.

Configuration

Setting up Fortisolator

The default IP address of the Fortisolator management interface is 192.168.1.99. To perform the initial configuration, connect a device to the management interface and configure the device with an IP address to 192.168.1.1/24. You can access Fortisolator using SSH or the Fortisolator GUI. The default username is **admin** and there is no default password.

Use the Fortisolator GUI or CLI to set the permanent IP address configuration.

You can perform the initial configuration using the serial console. For more information, see the [Fortisolator 1000F QuickStart Guide](#).

Configuring the console

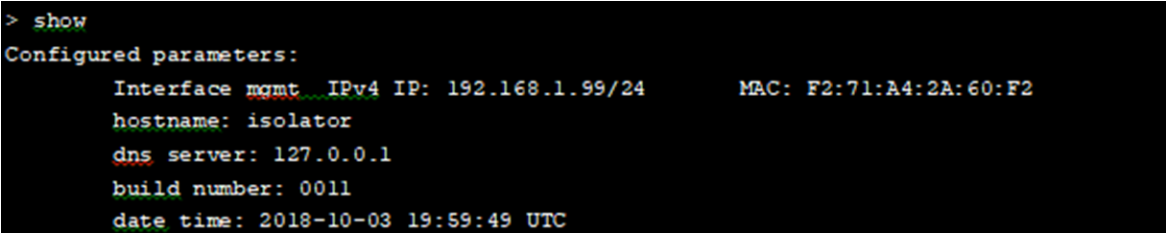
After the Fortisolator starts up, use the default console to complete initial interface configuration. By default, the management interface on Fortisolator (port3 on a VM installation) is set to 192.168.1.99.

The examples in this section are based on Fortisolator VM. The process is similar for other Fortisolator appliances, but interface settings can vary depending on the Fortisolator model.

Finding the current settings

To find the current settings on Fortisolator, type the `show` command in the Fortisolator CLI.

The following image shows an example of results from the `show` command:



```
> show
Configured parameters:
  Interface mgmt IPv4 IP: 192.168.1.99/24      MAC: F2:71:A4:2A:60:F2
  hostname: isolator
  dns server: 127.0.0.1
  build number: 0011
  date time: 2018-10-03 19:59:49 UTC
```

Setting the management IP address

To set the management IP address, type `set mgmt-ip <ip_address>/<subnet_mask>`. For example:

```
> set mgmt-ip 192.168.1.214/24
```

Setting the management gateway address

To set the management gateway, type `set mgmt-gw <subnet>/<gateway>`. For example:

```
> set mgmt-ip 0.0.0.0/0 192.168.1.254
```

All console commands

The following image shows the full list of console commands:

```

COM1 - Tera Term VT
File Edit Setup Control Window Help
>
> help
FortiIsolator Console
General:
  help      Display this text
  ?         Synonym for 'help'
  exit      Exit from the CLI
Configuration:
  show      Show bootstrap configuration
            Available attributes/values for show:

            ha-all          <null>
            ha-enabled       0/1
            ha-group-id      [1-255]
            ha-lost-threshold [1-60]
            ha-interval       [1-20]
                               in unit of 100ms
            ha-hello-holddown [5-300]
                               in unit of seconds
            ha-priority       [0-255]
                               255 means not used
            ha-allow-override 0/1
            ha-schedule       <schedule type>
            ha-virtual-ip     <IP/netmask>
                               e.g. 192.168.100.2/24
            ha-password       <PASSWORD>
            ha-password-enc   <Encoded PASSWORD>
            ha-interface      <Interface Name>
                               e.g. internal/external/mgmt

  show-ipmap-ha  Show HA ipmapping configuration
  set            Set configuration parameter
            Available attributes/values for set:

            internal-ip      <IP/netmask>
                               e.g. 192.168.100.2/24
            external-ip      <IP/netmask>
                               e.g. 192.168.100.2/24
            mgmt-ip          <IP/netmask>
                               e.g. 192.168.100.2/24
            date             <YYYY-MM-DD>
            time             <HH:MM:SS>
            dns              <pdns-ip sdns-ip>
                               e.g. 192.168.100.1 192.168.10.1
            ntp              <ntp-ip>
                               e.g. 192.168.100.1
            internal-gw      <SUBNET> <Gateway IP>
                               e.g. 192.168.100.0/24 192.168.100.1
            external-gw      <SUBNET> <Gateway IP>
                               e.g. 192.168.100.0/24 192.168.100.1
            mgmt-gw          <SUBNET> <Gateway IP>
                               e.g. 192.168.100.0/24 192.168.100.1
            hostname         <hostname>
            timezone         <timezone>
                               e.g. America/Los_Angeles
            ha-enabled       0/1
            ha-group-id      [1-255]
            ha-lost-threshold [1-60]
            ha-interval       [1-20]
                               in unit of 100ms
            ha-hello-holddown [5-300]
                               in unit of seconds
            ha-priority       [0-255]
                               255 means not used
            ha-allow-override 0/1
            ha-schedule       <schedule type>
            ha-virtual-ip     <IP/netmask>
                               e.g. 192.168.100.2/24
            ha-password       <PASSWORD>
            ha-password-enc   <Encoded PASSWORD>
            ha-interface      <Interface Name>
                               e.g. internal/external/mgmt
            fis-ipmap-ha      <priority external_isolator_ip internal_isolator_ip external_po
rt internal_port>
                               e.g. 0 192.168.100.1 10.1.0.1 12443 12887
            fis-ipmap        <external_port internal_port [external_isolator_ip]>
                               e.g. 12443 12887 192.168.100.1
            fis-ipmap-vip     <external_port internal_port external_isolator_ip>
                               e.g. 14443 14887 192.168.122.1

  unset        Unset configuration parameter
            Available attributes for unset:

            dns
            ntp
            internal-gw
            external-gw
            mgmt-gw
            fis-ipmap-ha
            fis-ipmap

```

```

COM1 - Tera Term VT
File Edit Setup Control Window Help

    ha-priority          [0-255]
                        255 means not used
    ha-allow-override    0/1
    ha-schedule           <schedule type>
    ha-virtual-ip         <IP/netmask>
                        e.g. 192.168.100.2/24
    ha-password          <PASSWORD>
    ha-password-enc       <Encoded PASSWORD>
    ha-interface         <Interface Name >
                        e.g. internal/external/mgmt

show-ipmap-ha           Show HA ipmapping configuration
set                     Set configuration parameter
                        Available attributes/values for set:

    internal-ip          <IP/netmask>
                        e.g. 192.168.100.2/24
    external-ip          <IP/netmask>
                        e.g. 192.168.100.2/24
    mgmt-ip              <IP/netmask>
                        e.g. 192.168.100.2/24
    date                 <YYYY-MM-DD>
    time                 <HH:MM:SS>
    dns                  <pdns-ip sdns-ip>
                        e.g. 192.168.100.1 192.168.10.1
    ntp                  <ntp-ip>
                        e.g. 192.168.100.1
    internal-gw           <SUBNET> <Gateway IP>
                        e.g. 192.168.100.0/24 192.168.100.1
    external-gw           <SUBNET> <Gateway IP>
                        e.g. 192.168.100.0/24 192.168.100.1
    mgmt-gw              <SUBNET> <Gateway IP>
                        e.g. 192.168.100.0/24 192.168.100.1
    hostname             <hostname>
    timezone             <timezone>
                        e.g America/Los_Angeles
    ha-enabled            0/1
    ha-group-id           [1-255]
    ha-lost-threshold     [1-60]
    ha-interval           [1-20]
                        in unit of 100ms
    ha-hello-holddown    [5-300]
                        in unit of seconds
    ha-priority           [0-255]
                        255 means not used
    ha-allow-override    0/1
    ha-schedule           <schedule type>
    ha-virtual-ip         <IP/netmask>
                        e.g. 192.168.100.2/24
    ha-password          <PASSWORD>
    ha-password-enc       <Encoded PASSWORD>
    ha-interface         <Interface Name >
                        e.g. internal/external/mgmt
    fis-ipmap-ha          <priority external_isolator_ip internal_isolator_ip external_po
rt internal_port>
                        e.g. 0 192.168.100.1 10.1.0.1 12443 12887
    fis-ipmap             <external_port internal_port [external_isolator_ip]>
                        e.g. 12443 12887 192.168.100.1
    fis-ipmap-vip         <external_port internal_port external_isolator_ip>
                        e.g. 14443 14887 192.168.122.1

unset                   Unset configuration parameter
                        Available attributes for unset:

    dns
    ntp
    internal-gw
    external-gw
    mgmt-gw
    fis-ipmap-ha
    fis-ipmap
    fis-ipmap-vip

System:
reboot                 Reboot the Fortisolator
system-upgrade          Upgrade Fortisolator System Image
factory-reset           Reset configuration to defaults and delete all data
shutdown               Shutdown the Fortisolator
status                 Display some status information
admin-pwd-reset         Reset Admin Password

Utilities:
nslookup               Basic tool for DNS debugging
ping                   Test network connectivity to another network host
fnsysctl disp           Display conf, category or log
fnsysctl tail          Display the last part of conf, category or log

Diagnostics:
hardware-info           Display general hardware status information
diagnose-nic            Display general network interface setting
diagnose-wf             Test and show WF action for an URL

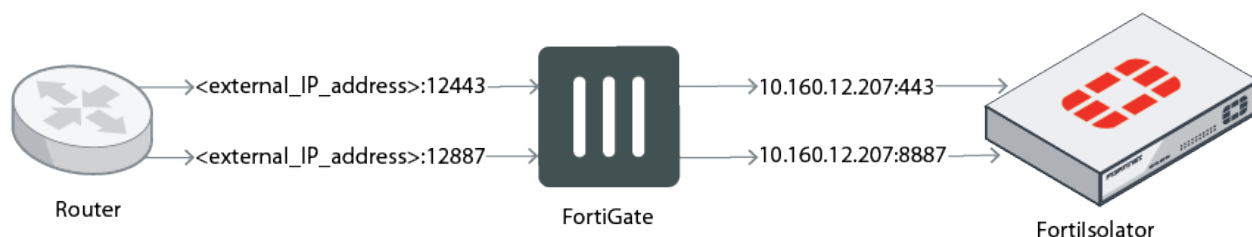
```

Port forwarding

Fortisolator supports IP mapping, which allows you to configure access to Fortisolator through port forwarding. Port forwarding maps external IP addresses to Fortisolator internal IP addresses. You can configure port forwarding in high availability (HA) or regular mode.

For example, if two networks, one external and one internal, connect to a FortiGate device, when IP addresses on the external network are accessed, traffic is redirected to the internal IP addresses on Fortisolator. The configuration information in this section follows an example setup with the following values:

External IP address of router	<external_IP_address>
Internal IP address of Fortisolator	10.160.12.207
Router redirections	<ul style="list-style-type: none"> • <external_IP_address>:12443 > 10.160.12.207:443 • <external_IP_address>:12887 > 10.160.12.207:8887



Configuring port forwarding in non-HA mode

FortiGate configuration

Complete the following steps in the FortiGate UI.

1. Go to **Policy & Objects > Virtual IPs**.
2. Create two IPv4 virtual IPs with the following information:
 - **IP-Mapping-443:** <external_IP_address> > 10.160.12.207 (TCP: 12443 > 443)
 - **IP-Mapping-8887:** <external_IP_address> > 10.160.12.207 (TCP: 12887 > 8887)

FortiGate VM64 FIS-FGT-IPMapping

Dashboard > + Create New Edit Clone Delete Search

Security Fabric >

FortiView >

Network >

System >

Policy & Objects >

- IPv4 Policy
- Authentication Rules
- IPv4 DoS Policy
- Addresses
- Wildcard FQDN Addresses
- Internet Service Database
- Services
- Schedules
- Virtual IPs** ☆
- IP Pools
- Protocol Options

Name	Details	Interfaces
IPv4 Virtual IP 5		
IP-Mapping-8888	--> 10.160.12.207 (TCP: 12888 --> 8888)	port1
IP-Mapping-443	--> 10.160.12.207 (TCP: 12443 --> 443)	port1
IP-Mapping-8887	--> 10.160.12.207 (TCP: 12887 --> 8887)	port1
IP-Mapping-Ha-443	--> 10.160.12.210 (TCP: 14443 --> 443)	port1
IP-Mapping-HA-8887	--> 10.160.12.210 (TCP: 14887 --> 8887)	port1

FortiGate VM64 FIS-FGT-IPMapping

Dashboard > Edit Virtual IP

Security Fabric >

FortiView >

Network >

System >

Policy & Objects >

- IPv4 Policy
- Authentication Rules
- IPv4 DoS Policy
- Addresses
- Wildcard FQDN Addresses
- Internet Service Database
- Services
- Schedules
- Virtual IPs** ☆
- IP Pools
- Protocol Options
- Traffic Shapers
- Traffic Shaping Policy
- Traffic Shaping Profile

VIP type IPv4

Name IP-Mapping-443

Comments Write a comment... 0/255

Color Change

Network

Interface port1

Type Static NAT

External IP address/range

Mapped IP address/range 10.160.12.207

Optional Filters

Port Forwarding

Protocol TCP UDP SCTP ICMP

External service port 12443

Map to port 443

OK Cancel

FortiGate VM64 FIS-FGT-IPMapping

Edit Virtual IP

VIP type: IPv4

Name: IP-Mapping-8887

Comments: Write a comment... 0/255

Color: Change

Network

Interface: port1

Type: Static NAT

External IP address/range:

Mapped IP address/range: 10.160.12.207

☐ Optional Filters

☒ Port Forwarding

Protocol: **TCP** UDP SCTP ICMP

External service port : 12887

Map to port: 8887

OK **Cancel**

3. Go to **Policy & Objects > IPv4 Policy > Create New**.

4. Create an IPv4 policy that includes the two virtual IPs that you created.

The screenshot shows the FortiGate VM64 configuration interface. The left sidebar displays the navigation menu with 'Policy & Objects' selected. The main area shows the 'Edit Policy' configuration for an IPv4 policy named 'p1->to->p2'. The configuration includes:

- Name:** p1->to->p2
- Incoming Interface:** port1
- Outgoing Interface:** port2
- Source:** all
- Destination:** IP-Mapping-443, IP-Mapping-8887
- Schedule:** always
- Service:** ALL
- Action:** ACCEPT (checked), DENY (unchecked)
- Inspection Mode:** Flow-based (checked), Proxy-based (unchecked)
- Firewall / Network Options:**
 - NAT:** enabled
 - IP Pool Configuration:** Use Outgoing Interface Address (checked)
 - Preserve Source Port:** unchecked
 - Protocol Options:** PROX (unchecked), default (checked)
- Security Profiles:**
 - AntiVirus: unchecked
 - Web Filter: unchecked
 - DNS Filter: unchecked
 - Application Control: unchecked
 - IPS: unchecked

The 'Select Entries' dialog is open, showing a list of entries. The entries include:

- ADDRESS (7)
- all
- FABRIC_DEVICE
- gmail.com
- login.microsoft.com
- login.microsoftonline.com
- login.windows.net
- none
- ADDRESS GROUP (1)
- Microsoft Office 365
- VIRTUAL IP/SERVER (5)
- IP-Mapping-443 (selected)
- IP-Mapping-8887 (selected)
- IP-Mapping-8888
- IP-Mapping-Ha-443
- IP-Mapping-HA-8887

FortiGate VM64FIS-FGT-IPMapping

admin

Interface Pair ViewBy Sequence

Dashboard

Security Fabric

FortiView

Network

System

Policy & Objects

IPv4 Policy

Authentication Rules

IPv4 DoS Policy

Addresses

Wildcard FQDN Addresses

Internet Service Database

Services

Schedules

Create NewEditDeletePolicy LookupSearch

Search

Interface Pair ViewBy Sequence

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
port1-->port2										
2	p1->to->p2	all	IP-Mapping-443 IP-Mapping-8887	always	ALL	ACCEPT	Enabled	UTM		5.26 GB
port2-->port1										
3	p2->to->p1	all	all	always	ALL	ACCEPT	Enabled	UTM		0 B
Implicit										
0	Implicit Deny	all	all	always	ALL	DENY		Disabled		566.60 MB

Fortisolator configuration

Use the Fortisolator CLI to configure port forwarding mappings. Use the `fis-ipmap` command in the following format:

```
set fis-ipmap <external_port> <internal_port> <external_IP_address>
```

For example, set `fis-ipmap 12443 12887 <external_IP_address>`

```
> set fis-ipmap 12443 12887 [REDACTED]
The apache will restart
httpd not running, trying to start
> show
Configured parameters:
  Interface    internal    IPv4 IP:      10.160.12.207/24    MAC: 00:0C:29:5F
:50:F1
  Interface    mgmt       IPv4 IP:      10.160.17.202/24    MAC: 00:0C:29:5F
:50:05
IPv4 Internal Gateway:      10.160.12.1
IPv4 MGMT Gateway :        10.160.17.1
hostname :                  N/A
dns server :                208.91.112.52
dns server :                172.30.1.105
build number :              0082(interim)
date time :                 2019-07-15 22:09:48 UTC
ip mapping :
mapping for port 443:        12443
mapping for port 8887:        12887
```

Client system configuration

Complete the following steps on the client system (for example, Windows 10).

1. In Windows 10, launch CMD as administrator.
2. Use the following commands to add the FortiGate IP address to the routing table on the client system:
 - a. At the command prompt, type `route ADD <external_IP_address> Mask 255.255.255.255 <FortiGate_IP_address>`.
 For example, `route -p ADD <external_IP_address> MASK 255.255.255.255 10.160.17.89`.

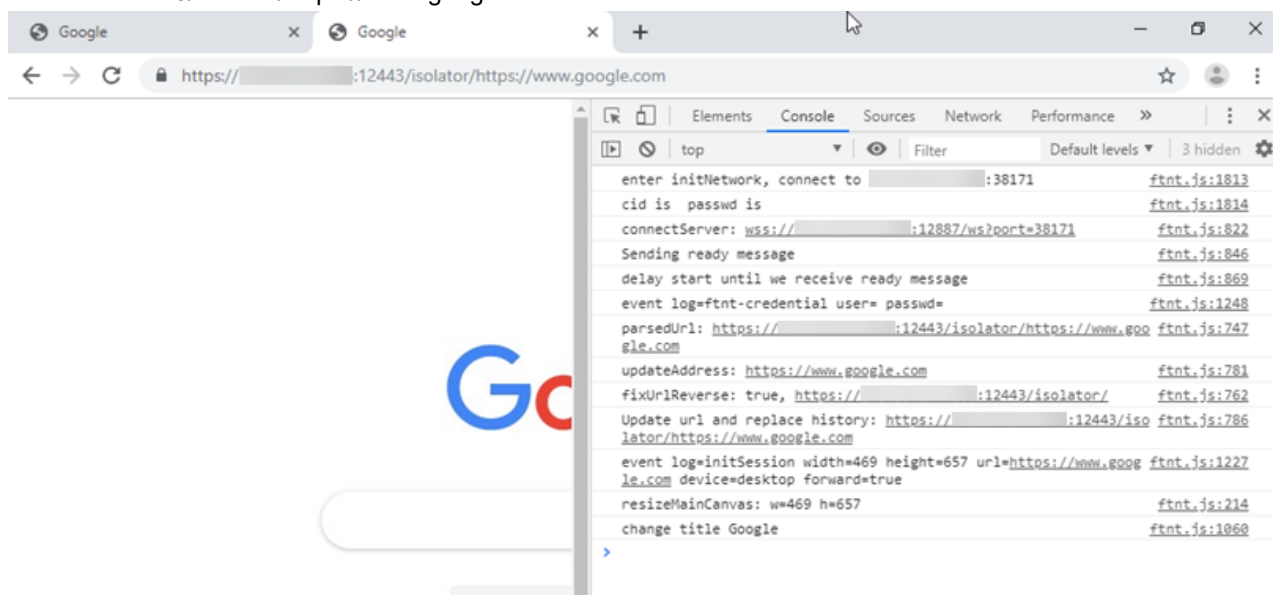
- b. To confirm the setup, type `route print`.

```
C:\WINDOWS\system32>route print

=====
Interface List
  5...00 0c 29 a2 fd 87 .....Intel(R) 82574L Gigabit Network Connection
  1.....Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
    0.0.0.0                0.0.0.0          10.160.17.1      10.160.17.205    25
   10.160.17.0            255.255.255.0    On-link          10.160.17.205    281
  127.255.255.255        255.255.255.255    On-link          127.0.0.1        331
  [redacted] 255.255.255.255  10.160.17.89     10.160.17.205    26
   224.0.0.0             240.0.0.0        On-link          127.0.0.1        331
   224.0.0.0             240.0.0.0        On-link          10.160.17.205    281
  255.255.255.255        255.255.255.255    On-link          127.0.0.1        331
  255.255.255.255        255.255.255.255    On-link          10.160.17.205    281
=====
Persistent Routes:
Network Address            Netmask          Gateway Address  Metric
  [redacted] 255.255.255.255    10.160.17.89     1
```

3. To verify that it works in a browser, browse to `https://<external_IP_address>:12443/isolator/https://www.google.com`.



Configuring port forwarding in HA mode

FortiGate configuration

Complete the following steps in the FortiGate UI.

1. Go to **Policy & Objects > Virtual IPs**.
2. Create two IPv4 virtual IPs with the following information:
 - **IP-Mapping-443**: <external_IP_address> > 10.160.12.207 (TCP: 14443 > 443)
 - **IP-Mapping-8887**: <external_IP_address> > 10.160.12.207 (TCP: 14887 > 8887)

FortiGate VM64 FIS-FGT-IPMapping

Dashboard > Security Fabric > FortiView > Network > System > **Policy & Objects**

IPv4 Policy
Authentication Rules
IPv4 DoS Policy
Addresses
Wildcard FQDN Addresses
Internet Service Database
Services
Schedules
Virtual IPs ☆
IP Pools
Protocol Options
Traffic Shapers
Traffic Shaping Policy

+ Create New Edit Clone Delete Search

Name	Details	Interfaces
IPv4 Virtual IP 5		
IP-Mapping-8888	--> 10.160.12.207 (TCP: 12888 --> 8888)	port1
IP-Mapping-443	--> 10.160.12.207 (TCP: 12443 --> 443)	port1
IP-Mapping-8887	--> 10.160.12.207 (TCP: 12887 --> 8887)	port1
IP-Mapping-Ha-443	--> 10.160.12.210 (TCP: 14443 --> 443)	port1
IP-Mapping-HA-8887	--> 10.160.12.210 (TCP: 14887 --> 8887)	port1

FortiGate VM64 FIS-FGT-IPMapping

Dashboard > Security Fabric > FortiView > Network > System > **Policy & Objects**

IPv4 Policy
Authentication Rules
IPv4 DoS Policy
Addresses
Wildcard FQDN Addresses
Internet Service Database
Services
Schedules
Virtual IPs ☆
IP Pools
Protocol Options
Traffic Shapers

Edit Virtual IP

VIP type IPv4

Name IP-Mapping-Ha-443

Comments Write a comment... 0/255

Color Change

Network

Interface port1

Type Static NAT

External IP address/range

Mapped IP address/range 10.160.12.210

Optional Filters

Port Forwarding

Protocol TCP UDP SCTP ICMP

External service port 14443

Map to port 443

FortiGate VM64 FIS-FGT-IPMapping

Policy & Objects

- Dashboard
- Security Fabric
- FortiView
- Network
- System
- Policy & Objects**
- IPv4 Policy
- Authentication Rules
- IPv4 DoS Policy
- Addresses
- Wildcard FQDN Addresses
- Internet Service Database
- Services
- Schedules
- Virtual IPs**
- IP Pools
- Protocol Options
- Traffic Shapers

Edit Virtual IP

VIP type: IPv4

Name: IP-Mapping-HA-8887

Comments: Write a comment... 0/255

Color: Change

Network

Interface: port1

Type: Static NAT

External IP address/range:

Mapped IP address/range: 10.160.12.210

☐ Optional Filters

☒ Port Forwarding

Protocol: **TCP** UDP SCTP ICMP

External service port: 14887

Map to port: 8887

3. Go to **Policy & Objects > IPv4 Policy > Create New**.

4. Create an IPv4 policy that includes the two virtual IPs that you created.

FortiGate VM64 FIS-FGT-IPMapping

Edit Policy

Name: p1->to->p2

Incoming Interface: port1

Outgoing Interface: port2

Source: all

Destination: IP-Mapping-Ha-443, IP-Mapping-HA-8887

Schedule: always

Service: ALL

Action: ACCEPT

Inspection Mode: Flow-based

Firewall / Network Options

NAT: ☒ NAT

IP Pool Configuration: Use Outgoing Interface Address

Preserve Source Port: ☐

Protocol Options: PRX default

Security Profiles

AntiVirus: ☐

Web Filter: ☐

DNS Filter: ☐

Application Control: ☐

IPS: ☐

Select Entries

Address: all, FABRIC_DEVICE, gmail.com, login.microsoft.com, login.microsoftonline.com, login.windows.net, none

Internet Service: ADDRESS GROUP (1), Microsoft Office 365, VIRTUAL IP/SERVER (5), IP-Mapping-443, IP-Mapping-8887, IP-Mapping-Ha-443, IP-Mapping-HA-8887

Close

OK Cancel

FortiGate VM64 FIS-FGT-IPMapping

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles
1	port1 -> port2	all	IP-Mapping-Ha-443, IP-Mapping-HA-8887	always	ALL	ACCEPT	Enabled	
2	p1->to->p2	all	IP-Mapping-Ha-443, IP-Mapping-HA-8887	always	ALL	ACCEPT	Enabled	
3	port2 -> port1	all	all	always	ALL	ACCEPT	Enabled	
0	Implicit Deny	all	all	always	ALL	DENY		

Fortisolator configuration

Use the Fortisolator CLI to configure port forwarding mappings. Use the following commands:

1. `set fis-ipmap <port_map_to_443> <port_map_to_8887> <external_IP_address>`
For example, set `fis-ipmap 12443 12887 <external_IP_address>`.

```
> set fis-ipmap 12443 12887 [REDACTED]
The apache will restart
httpd not running, trying to start
> show
Configured parameters:
      Interface    internal    IPv4 IP:    10.160.12.207/24    MAC: 00:0C:29:5F
:50:F1
      Interface    mgmt      IPv4 IP:    10.160.17.202/24    MAC: 00:0C:29:5F
:50:05
IPv4 Internal Gateway:    10.160.12.1
IPv4 MGMT Gateway :    10.160.17.1
hostname :    N/A
dns server :    208.91.112.52
dns server :    172.30.1.105
build number :    0082(interim)
date time :    2019-07-15 22:09:48 UTC
ip mapping :
mapping for port 443:    12443
mapping for port 8887:    12887
```

2. `set fis-ipmap-vip <port_map_to_443> <port_map_to_8887> <external_IP_address>`
For example, set `fis-ipmap-vip 14443 14887 <external_IP_address>`.

```
> set fis-ipmap-vip 14443 14887 [REDACTED]
> show
Configured parameters:
      Interface    internal    IPv4 IP:    10.160.12.207/24    MAC: 00:0C:29:5F
:50:F1
      Interface    mgmt      IPv4 IP:    10.160.17.202/24    MAC: 00:0C:29:5F
:50:05
IPv4 Internal Gateway:    10.160.12.1
IPv4 MGMT Gateway :    10.160.17.1
hostname :    N/A
dns server :    208.91.112.52
dns server :    172.30.1.105
build number :    0082(interim)
date time :    2019-07-15 23:05:47 UTC
ip mapping :
mapping for port 443:    12443
mapping for port 8887:    12887
ip mapping (VIP) :
mapping for port 443 (VIP):    14443
mapping for port 8887 (VIP):    14887
> _
```

3. `set fis-ipmap-ha <priority> <external_IP_address> <internal_IP_address:slave_1> <port_map_to_443> <port_map_to_8887>`
For example, set `fis-ipmap-ha 10 <external_IP_address> 10.160.12.207 12443 12887`

```

> set fis-ipmap-ha 10 [REDACTED] 10.160.12.207 12443 12887
> show
Configured parameters:
Interface      internal      IPv4 IP:      10.160.12.207/24      MAC: 00:0C:29:5F
:50:F1
Interface      mgmt         IPv4 IP:      10.160.17.202/24      MAC: 00:0C:29:5F
:50:05
IPv4 Internal Gateway:      10.160.12.1
IPv4 MGMT Gateway      :      10.160.17.1
hostname      :      N/A
dns server      :      208.91.112.52
dns server      :      172.30.1.105
build number      :      0082(interim)
date time      :      2019-07-15 23:54:44 UTC
ip mapping      :
mapping for port 443:      12443
mapping for port 8887:      12887
ip mapping (VIP)      :
mapping for port 443 (VIP):      14443
mapping for port 8887 (VIP):      14887
> _

```

Client system configuration

Complete the following steps on the client system (for example, Windows 10).

1. In Windows 10, launch CMD as administrator.
2. Use the following commands to add the FortiGate IP address to the routing table on the client system:
 - a. At the command prompt, type `route ADD <external_IP_address> Mask 255.255.255.255 <FortiGate_IP_address>`.
 For example, `route -p ADD <external_IP_address> MASK 255.255.255.255 10.160.17.89`.

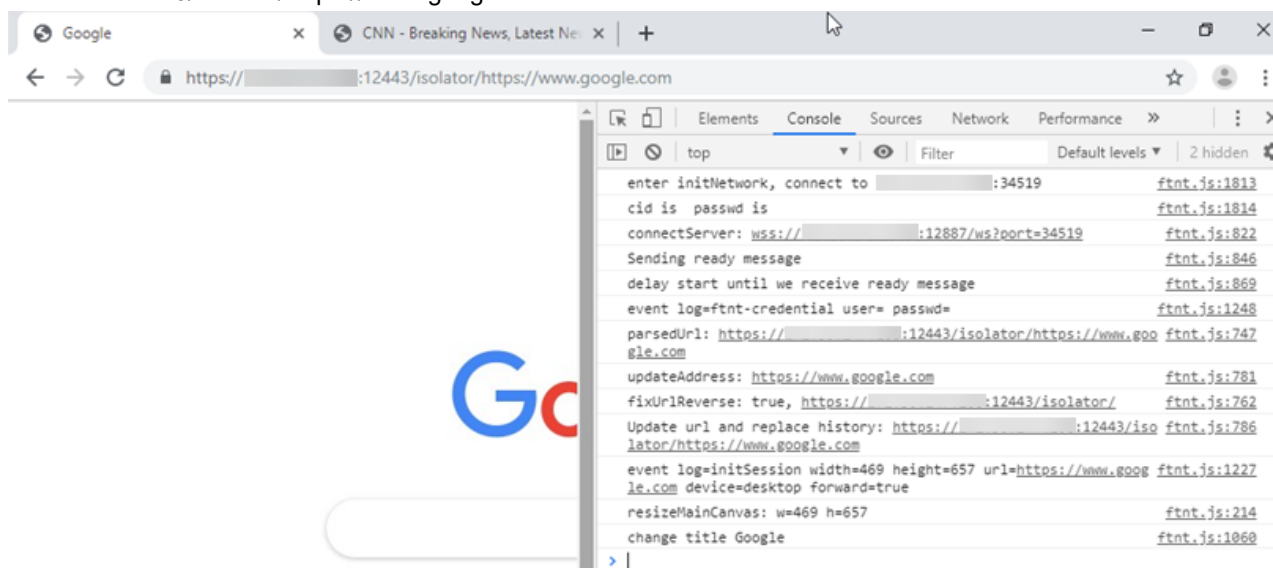
- b. To confirm the setup, type `route print`.

```
C:\WINDOWS\system32>route print

=====
Interface List
  5...00 0c 29 a2 fd 87 .....Intel(R) 82574L Gigabit Network Connection
  1.....Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
  Network Destination        Netmask          Gateway          Interface        Metric
  0.0.0.0                    0.0.0.0          10.160.17.1      10.160.17.205    25
  10.160.17.0                255.255.255.0    On-link          10.160.17.205    281
  127.255.255.255            255.255.255.255  On-link          127.0.0.1        331
  [redacted] 255.255.255.255    10.160.17.89     10.160.17.205    26
  224.0.0.0                  240.0.0.0        On-link          127.0.0.1        331
  224.0.0.0                  240.0.0.0        On-link          10.160.17.205    281
  255.255.255.255            255.255.255.255  On-link          127.0.0.1        331
  255.255.255.255            255.255.255.255  On-link          10.160.17.205    281
=====
Persistent Routes:
  Network Address          Netmask          Gateway Address  Metric
  [redacted] 255.255.255.255  10.160.17.89     1
=====
```

3. To verify that it works in a browser, browse to `https://<external_IP_address>:14443/isolator/https://www.google.com`.



Getting started in the Fortisolator UI

Logging in to the Fortisolator UI

Use this procedure to log in to the Fortisolator UI.

Steps

1. Open a web browser and go to `http://<management_IP_address>`.
 - where `<management_IP_address>` is the IP address that you configured for the management interface. The default is 192.168.199.
2. Type your username and password.
Log in to the Fortisolator UI. The default username is **admin** and there is no default password.
3. Click **Login**.

Configuring time settings

Use this procedure to configure time settings for Fortisolator.

Steps

1. In the Fortisolator UI, click **Dashboard**, and find the **System Information** widget.
2. In the **System Time** field, click **Change**.
3. In the **Time Zone** drop-down list, select the time zone.
4. Set the time by doing one of the following tasks:
 - To set the time manually, select **Set Time**, and select the time and date options in the drop-down lists.
 - To configure an NTP server, select **Synchronize with NTP Server** and enter the IP address of the NTP server.
5. Click **Apply**.

Changing the administrator password

Use this procedure to change the administrator password for Fortisolator.

Steps



1. In the top-right corner of the Fortisolator UI, click your username (for example, admin).
2. Click **Change Password**.
3. In the **Password** field, type the new password.
4. In the **Confirm Password** field, type the new password again.
5. Click **OK**.

Configuring interface settings

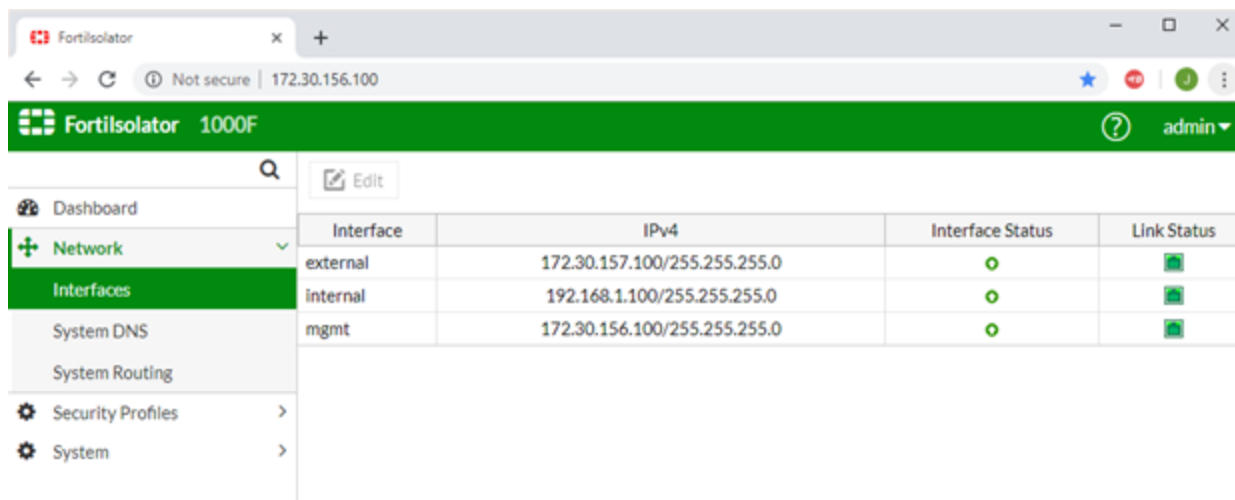
Use this procedure to configure Fortisolator interface settings.

Steps

1. In the Fortisolator UI, go to **Network > Interfaces**.
2. To edit an interface, select the interface in the table, and click **Edit**.

3. To change the interface status, set the **Interface Status** field to one of the following options:
 - To turn on the interface, click **Link Up** .
 - To turn off the interface, click **Link Down** .
4. To change the IP address of the interface, enter an IP address and netmask in the **IPv4** field.
5. Click **OK**.

The following image shows an example of the Fortisolator **Interfaces** page.



Configuring DNS settings

Use this procedure to configure DNS settings for Fortisolator.

Steps

1. In the Fortisolator UI, go to **Network > System DNS**.
2. Type the IP address of the **Primary DNS Server**.
3. Type the IP address of the **Secondary DNS Server**.
4. Click **OK**.

Configuring routing settings

Use this procedure to configure routing settings for Fortisolator.

Adding a static route

Use this procedure to add a static route.

Steps

1. In the Fortisolator UI, go to **Network > System Routing**.
2. To add a new static route, click **Create New**.

3. Type the destination IP address and subnet mask in the **Destination IP/Mask** field.
4. Type the gateway IP address in the **Gateway** field.
5. In the **Device** drop-down list, select the interface for the static route.
6. Click **OK**.

Editing a static route

Use this procedure to edit a static route.

Steps

1. In the Fortisolator UI, go to **Network > System Routing**.
2. To edit an existing static route, select the interface in the table, and click **Edit**.
3. Type the destination IP address and subnet mask in the **Destination IP/Mask** field.
4. Type the gateway IP address in the **Gateway** field.
5. In the **Device** drop-down list, select the interface for the static route.
6. Click **OK**.

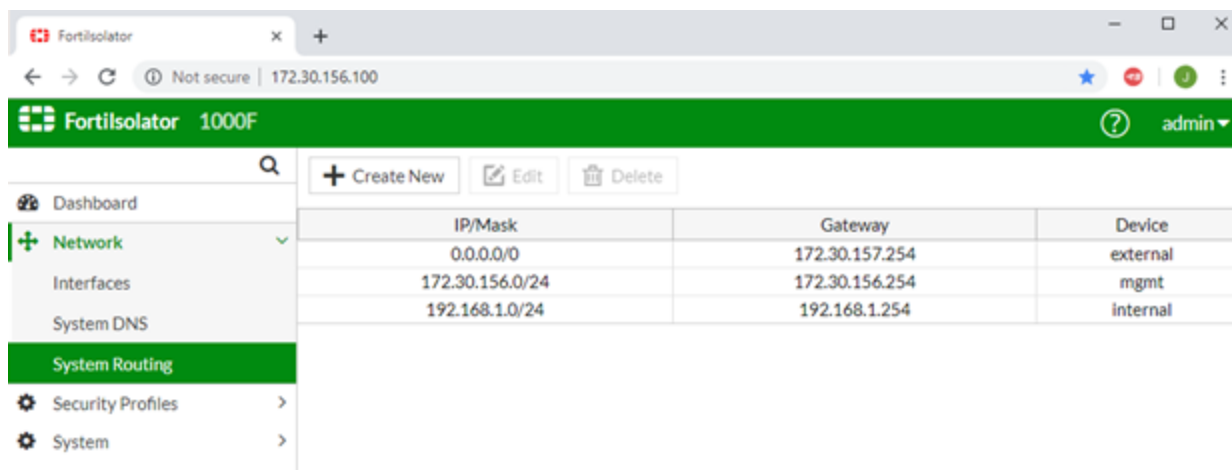
Deleting a static route

Use this procedure to delete a static route.

Steps

1. In the Fortisolator UI, go to **Network > System Routing**.
2. To delete a static route, select the interface in the table, and click **Delete**.

The following image shows an example of the **System Routing** page.



Configuring web filter profiles

Fortisolator supports web filtering, which allows you to control the webpages that users can view. You can block specific URLs or websites, which then prevents a user's browser from loading webpages from these websites.

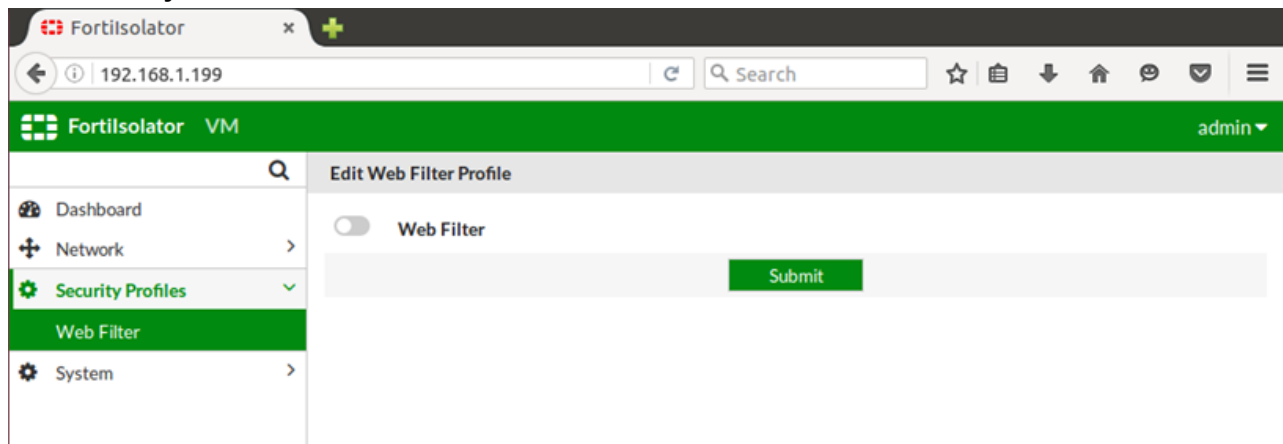
Use this procedure to configure web filter profiles on Fortisolator.

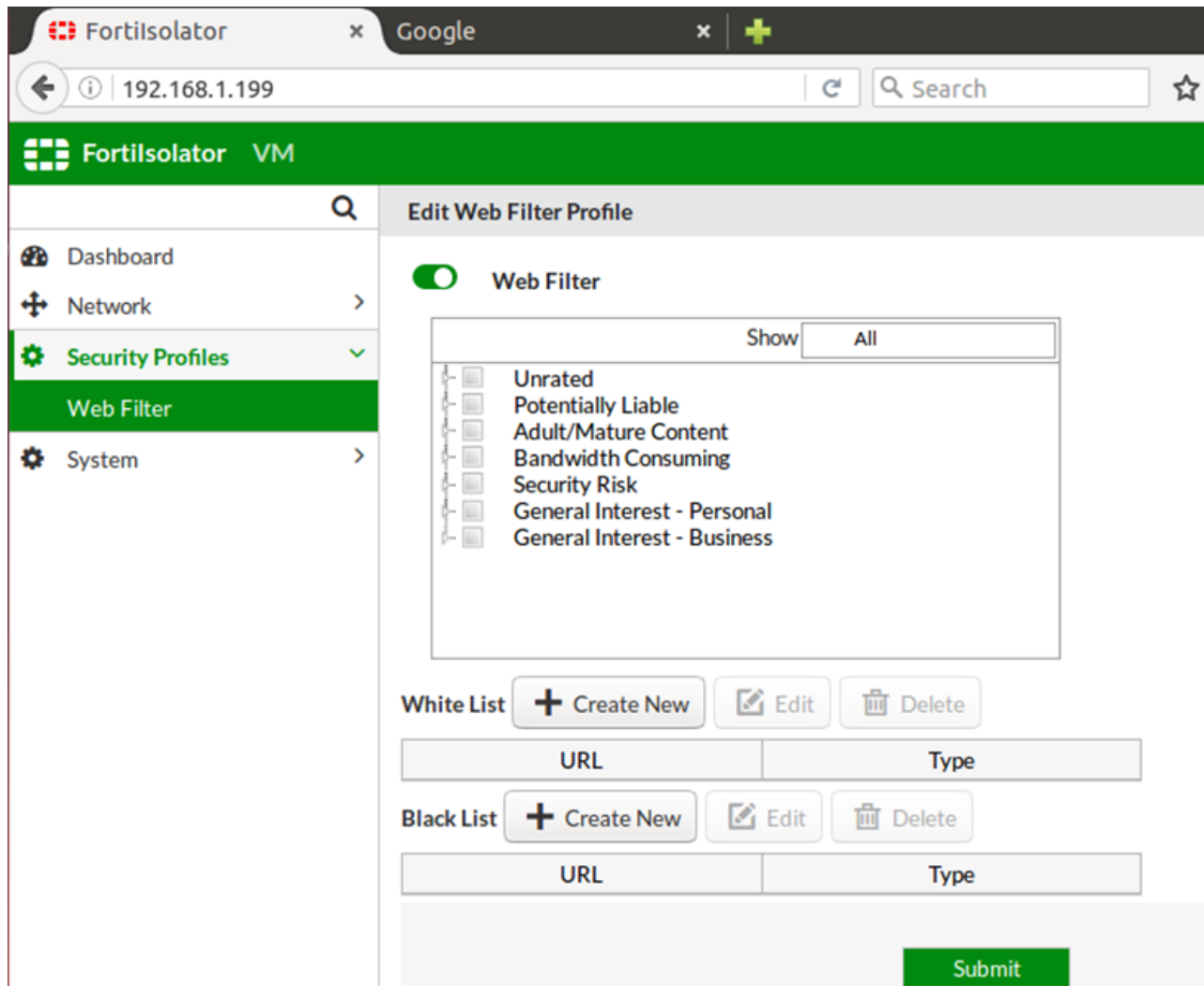
Prerequisites

- Ensure that Fortisolator has a valid license installed.
- Register the device to a production server: <https://support.fortinet.com/product/RegistrationEntry.aspx>.
- Ensure that the IP address in the Fortisolator license is the same as the Fortisolator management IP address.

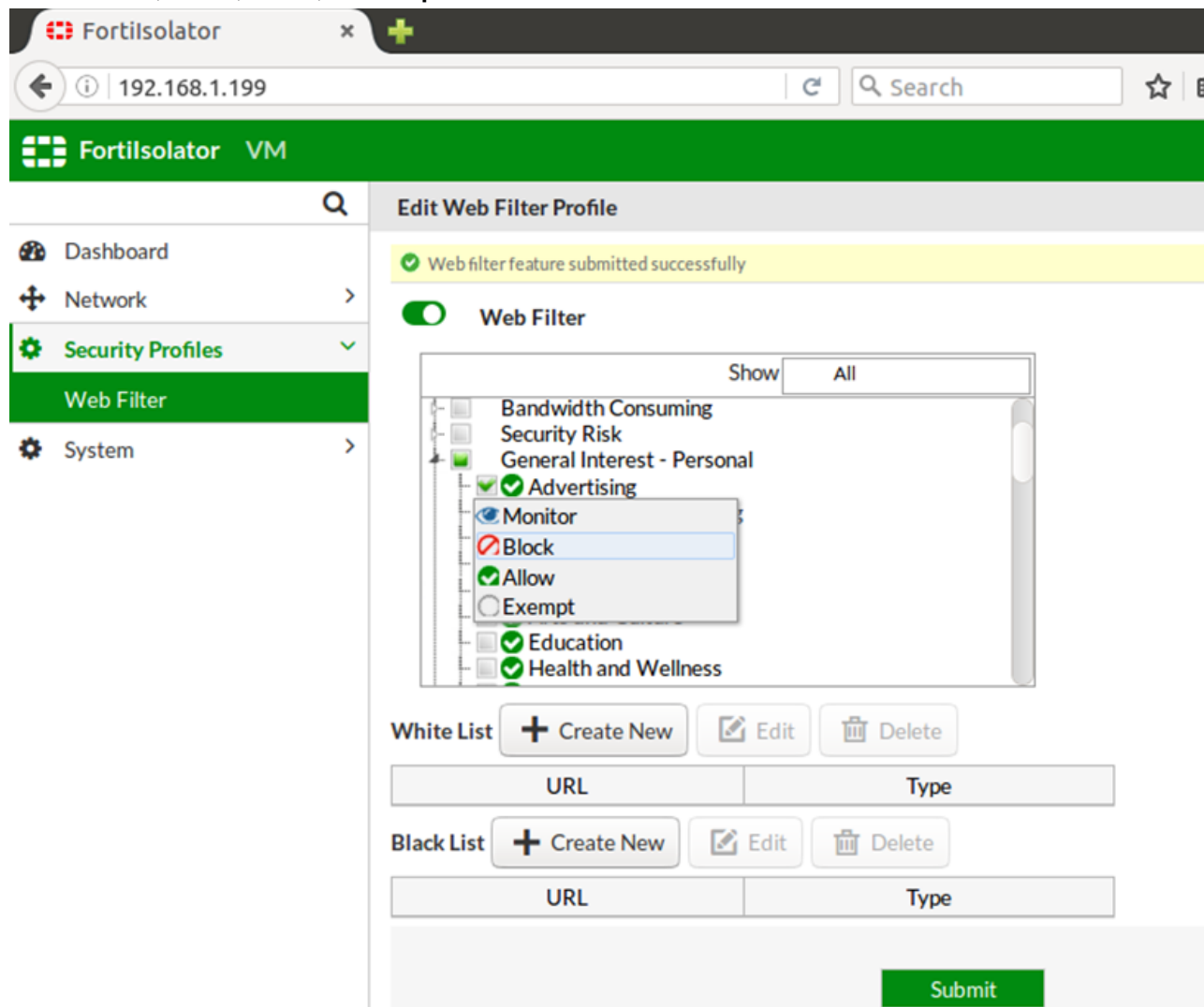
Steps

1. Go to **Security Profiles > Web Filter**.

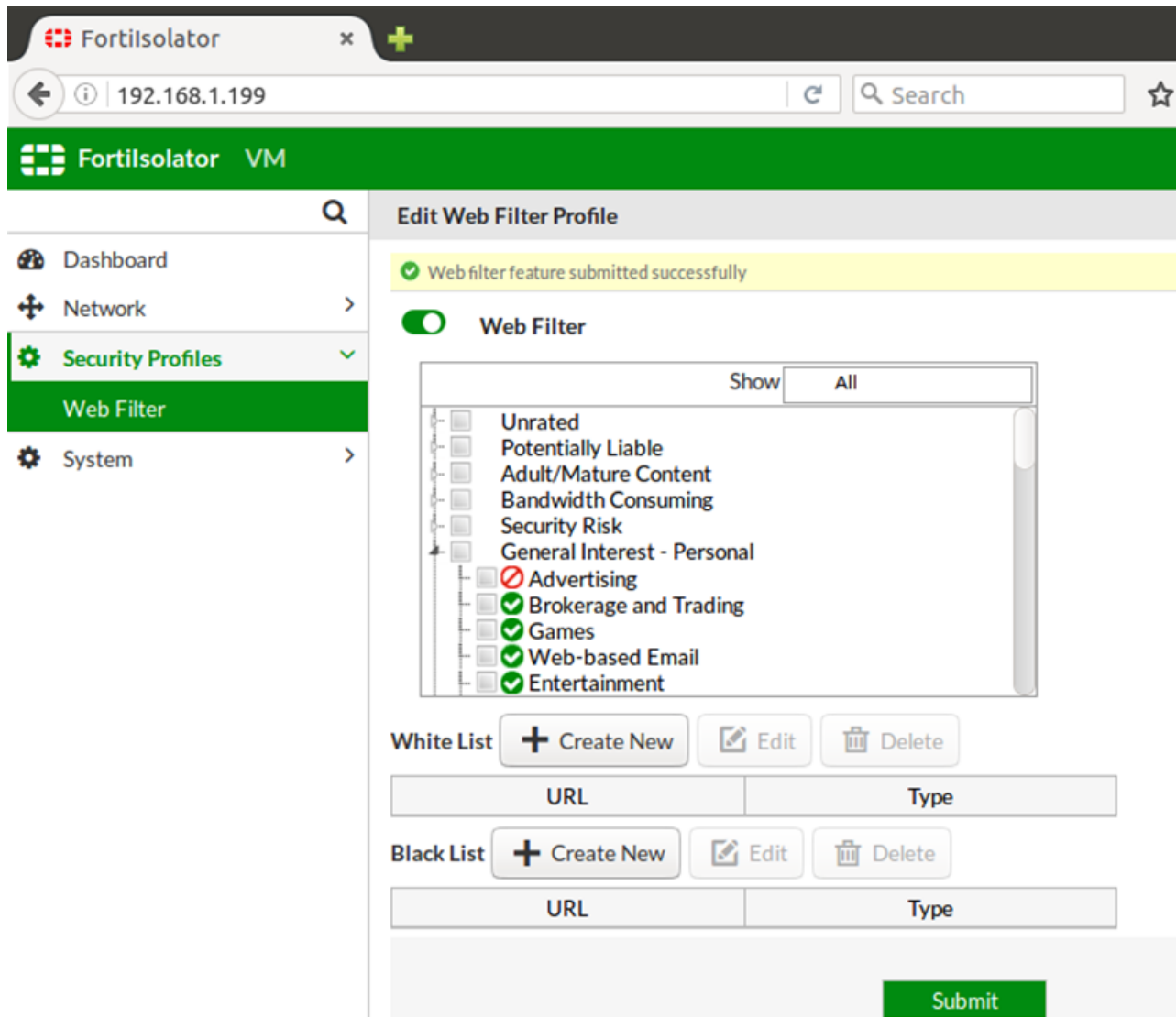


2. Enable Web Filter.**3. To set web filters for categories, in the web filter list, expand a category, and then a subcategory.**

4. Click **Monitor**, **Block**, **Allow**, or **Exempt**.



The symbols beside the subcategories show the web filter action that you configured.



5. To set web filters for specific websites, in the **White List** or **Black List** sections, click **Create New**.
6. Type the URL, click a filter type, and click **OK**.
The **URL** and **Type** that you configured is displayed in the **White List** or **Black List** tables.

The screenshot shows the Fortisolator web interface. The browser address bar displays '192.168.1.199'. The left sidebar contains a navigation menu with 'Dashboard', 'Network', 'Security Profiles', 'Web Filter', and 'System'. The 'Web Filter' option is selected and highlighted in green. The main content area is titled 'Edit Web Filter Profile'. A yellow notification bar at the top of the main area states 'Web filter feature submitted successfully'. Below this, there is a 'Web Filter' toggle switch which is turned on. A list of categories is displayed with checkboxes: 'Unrated', 'Potentially Liable', 'Adult/Mature Content', 'Bandwidth Consuming', 'Security Risk', 'General Interest - Personal', 'Advertising' (unchecked), 'Brokerage and Trading' (checked), 'Games' (checked), 'Web-based Email' (checked), and 'Entertainment' (checked). Below the list, there are sections for 'White List' and 'Black List'. Each section has a '+ Create New' button and 'Edit' and 'Delete' buttons. The 'Black List' section contains a table with one entry: 'www.yahoo.com' with a 'Simple' type. A green 'Submit' button is located at the bottom right of the page.

Fortisolator VM

Dashboard

Network

Security Profiles

Web Filter

System

Edit Web Filter Profile

Web filter feature submitted successfully

☒ Web Filter

Show All

- ☐ Unrated
- ☐ Potentially Liable
- ☐ Adult/Mature Content
- ☐ Bandwidth Consuming
- ☐ Security Risk
- ☐ General Interest - Personal
- ☐ Advertising
- ☒ Brokerage and Trading
- ☒ Games
- ☒ Web-based Email
- ☒ Entertainment

White List + Create New Edit Delete

URL	Type
-----	------

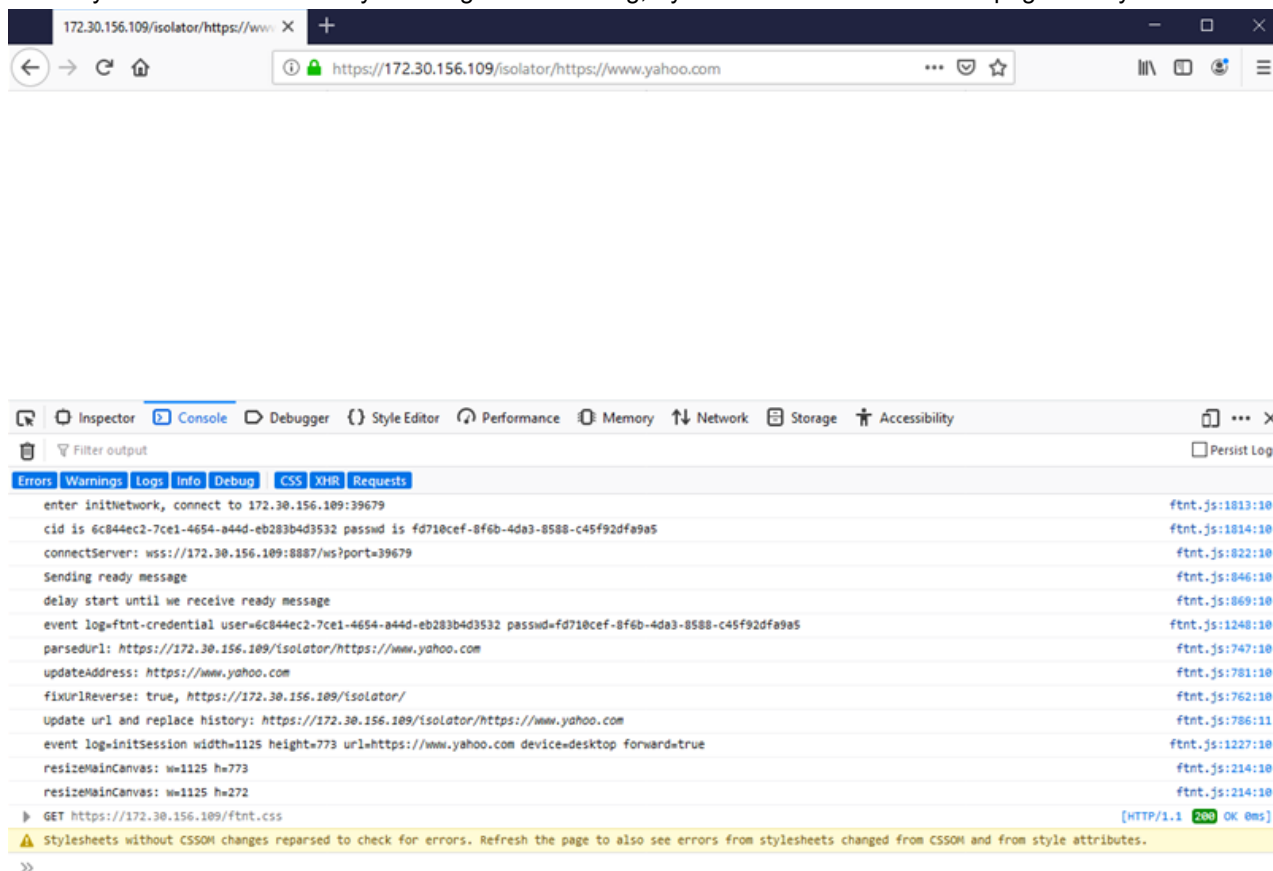
Black List + Create New Edit Delete

URL	Type
www.yahoo.com	Simple

Submit

7. Click **Submit**.

8. To verify that the web filter that you configured is working, try to browse to one of the webpages that you blocked.

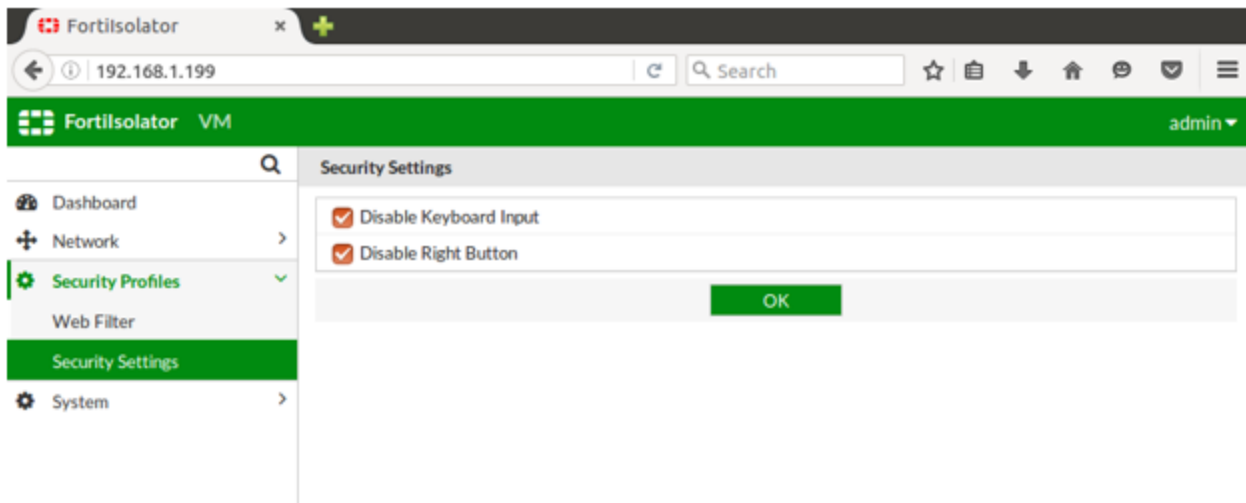


Configuring security settings

You can configure the following security settings in FortiIsolator:

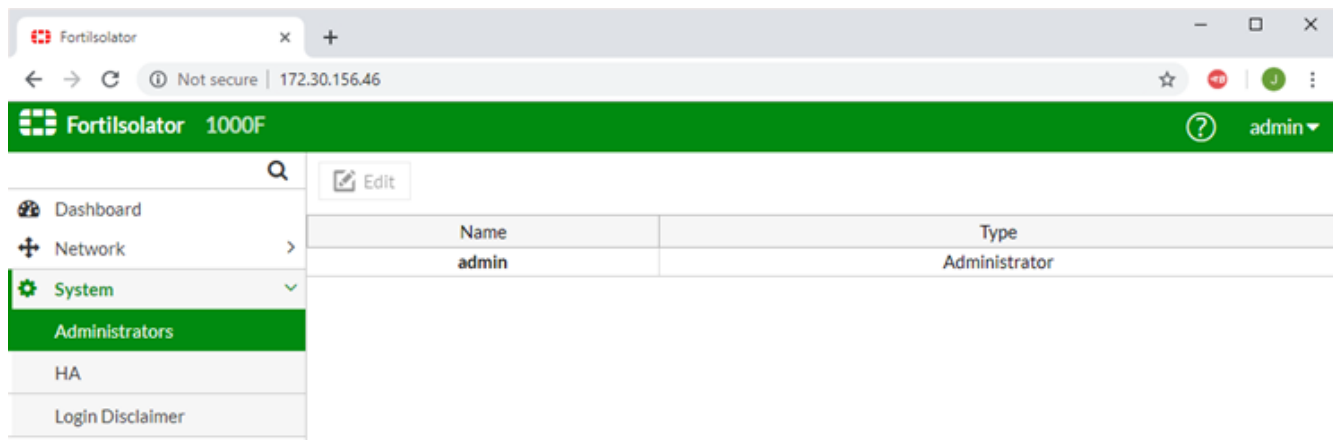
- **Disable Keyboard Input:** When you select this setting, users cannot type any characters using their keyboard, including the space bar and `Enter` key. However, they can continue to use arrow keys (up, down, left, or right) to navigate through pages in their web browser.
- **Disable Right Button:** When you select this setting, you disable the right button on the computer mouse. When users right-click, the web browser does not respond and menu items do not show. The left button will continue to work as usual.

To configure security settings, go to **Security Profiles > Security Settings**.



Configuring administrator settings

To configure administrator settings, go to **System > Administrators**.



Configuring high availability

Fortisolator supports high availability and A-A clustering. You can deploy devices in a cluster, and distribute traffic using Round Robin or Weighted Round Robin load balancing. You can use the Fortisolator UI or Fortisolator CLI to configure high availability.

Fortisolator UI

To configure high availability, go to **System > HA**.

Fortisolator 1000F

HA Settings

Note: The Fortisolator will reboot after the HA settings are changed

Enable/Disable: ☐

Virtual IP:

Priority:

Cluster Settings

Group Id:

Password: Change

Allow Override: ☐

Schedule Type:

Interface Name	Lost Threshold	Hello Holddown	Interval
<input type="text" value="internal"/>	<input type="text" value="10"/>	<input type="text" value="5"/>	<input type="text" value="10"/>

Apply

Fortisolator CLI

To configure high availability, use the following CLI commands:

```

ha-enabled 0/1
ha-group-id [1-255]
ha-lost-threshold [1-60]
ha-interval [1-20]
in unit of 100ms
ha-hello-holddown [5-300]
in unit of seconds
ha-priority [0-255]
255 means not used
ha-allow-override 0/1
ha-schedule <schedule type>
ha-virtual-ip <IP/netmask>
e.g. 192.168.100.2/24
ha-password <PASSWORD>
ha-password-enc <Encoded PASSWORD>
ha-interface <Interface Name >
e.g. internal/external/mgmt

```

After you enable or disable high availability, you must restart Fortisolator.

```

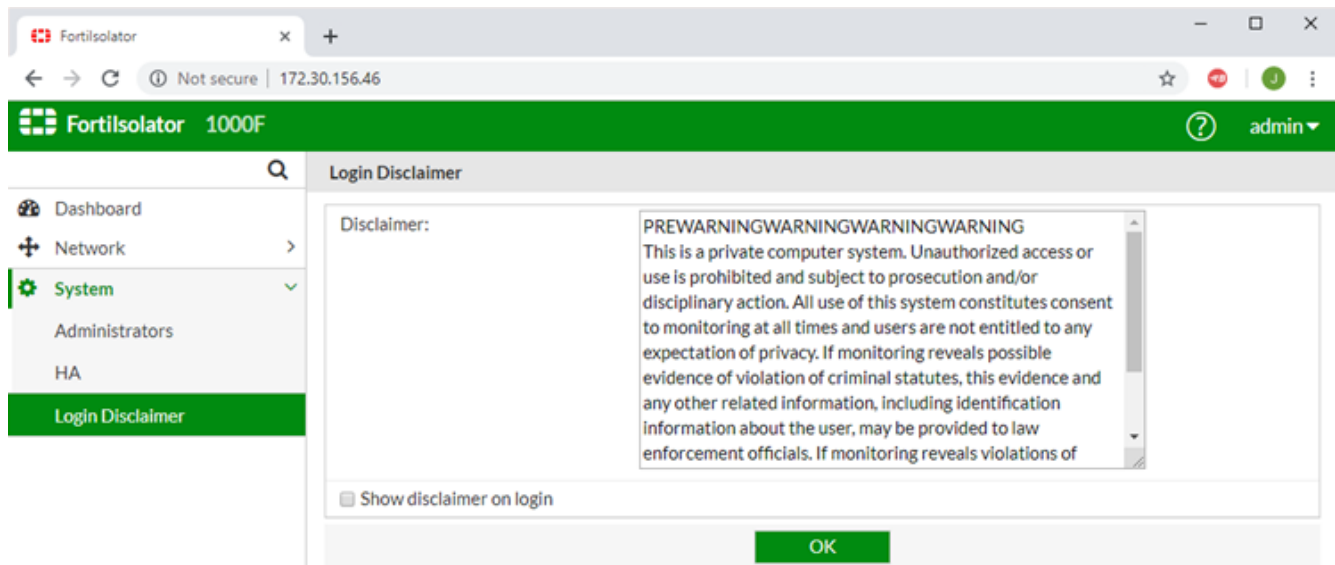
VT COM1 - Tera Term VT
File Edit Setup Control Window Help

Welcome to Isolator
Fortisolator login:
Welcome to Isolator
Fortisolator login: admin
Password:
> show
Configured parameters:
  Interface internal IPv4 IP: [REDACTED]/22 MAC: 00:90:0B:70:EC:E2
  Interface mgmt IPv4 IP: [REDACTED]/24 MAC: 00:90:0B:6D:A3:2F
IPv4 Internal Gateway:
hostname : FortiIsolator
dns server :
dns server :
build number : 0082<interim>
date time : 2019-07-15 12:01:16 PDT
ip mapping <VIP> :
mapping for port 443 <VIP>: 12443
mapping for port 8887 <VIP>: 12887
> show
Configured parameters:
  Interface internal IPv4 IP: [REDACTED]/22 MAC: 00:90:0B:70:EC:E2
  Interface mgmt IPv4 IP: [REDACTED]/24 MAC: 00:90:0B:6D:A3:2F
IPv4 Internal Gateway:
hostname : FortiIsolator
dns server :
dns server :
build number : 0082<interim>
date time : 2019-07-15 12:01:21 PDT
ip mapping <VIP> :
mapping for port 443 <VIP>: 12443
mapping for port 8887 <VIP>: 12887
> show ha-all
ha enabled : Enabled
ha gid : 30
ha lost threshold : 7
ha interval : 7
ha holddown : 5
ha priority : 50
ha allow override : 0
ha schedule : Round Robin
ha vip : [REDACTED]
ha password :
ha interface : internal
> set ha-enabled
[0]Disabled
[1]Enabled
[2]Duplicated
Please choose the value(0 to 2):0
The ha enabled is set as "Disabled"
Warning: FortiIsolator will need reboot after the HA settings are changed
> █

```

Configuring the login disclaimer

To configure a login disclaimer, go to **System > Login Disclaimer**.



Operation

Run web browsers through Fortisolator

You can run web browsers through Fortisolator in the following modes:

- IP forwarding mode
- Proxy mode
- PAC file mode

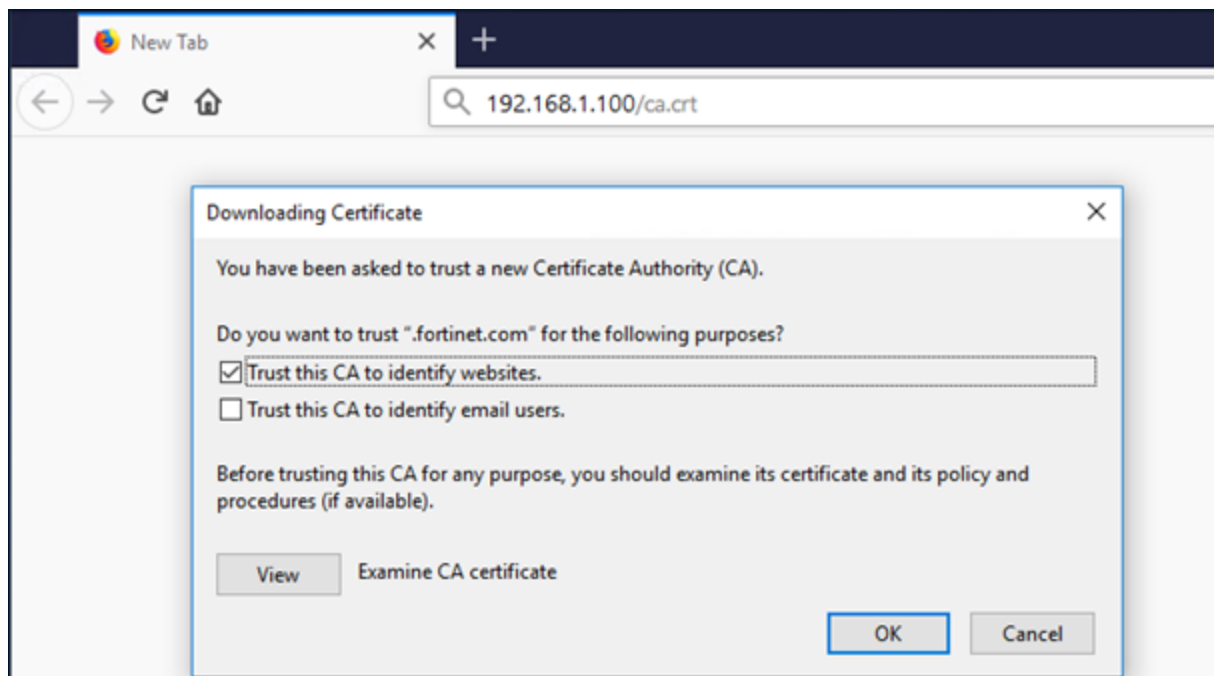
IP forwarding mode

Using IP forwarding mode with Mozilla Firefox

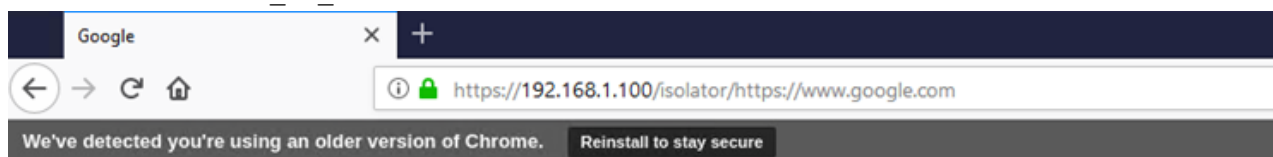
Use this procedure to configure IP forwarding mode with Mozilla Firefox.

Steps

1. To download the Fortisolator certificate (ca.crt) and import it into the Mozilla Firefox browser, follow these steps:
 - a. In the Mozilla Firefox browser address bar, type `http://<internal_IP_address>/ca.crt` (for example, `http://192.168.1.100/ca.crt`).
 - where `<internal_IP_address>` is the IP address of the Fortisolator internal interface. For example, the IP address of the internal interface that you configured in step 3 of [Fortisolator appliance installation on page 7](#).
 - b. In the **Downloading Certificate** window, select the **Trust this CA to identify websites** checkbox.
 - c. Click **OK**



2. In the Mozilla Firefox browser address bar, type `https://<internal_IP_address>/isolator/https://www.google.com` (for example, `https://192.168.1.100/isolator/https://www.google.com`).
- where `<internal_IP_address>` value is the IP address of the Fortisolator internal interface



Google Search

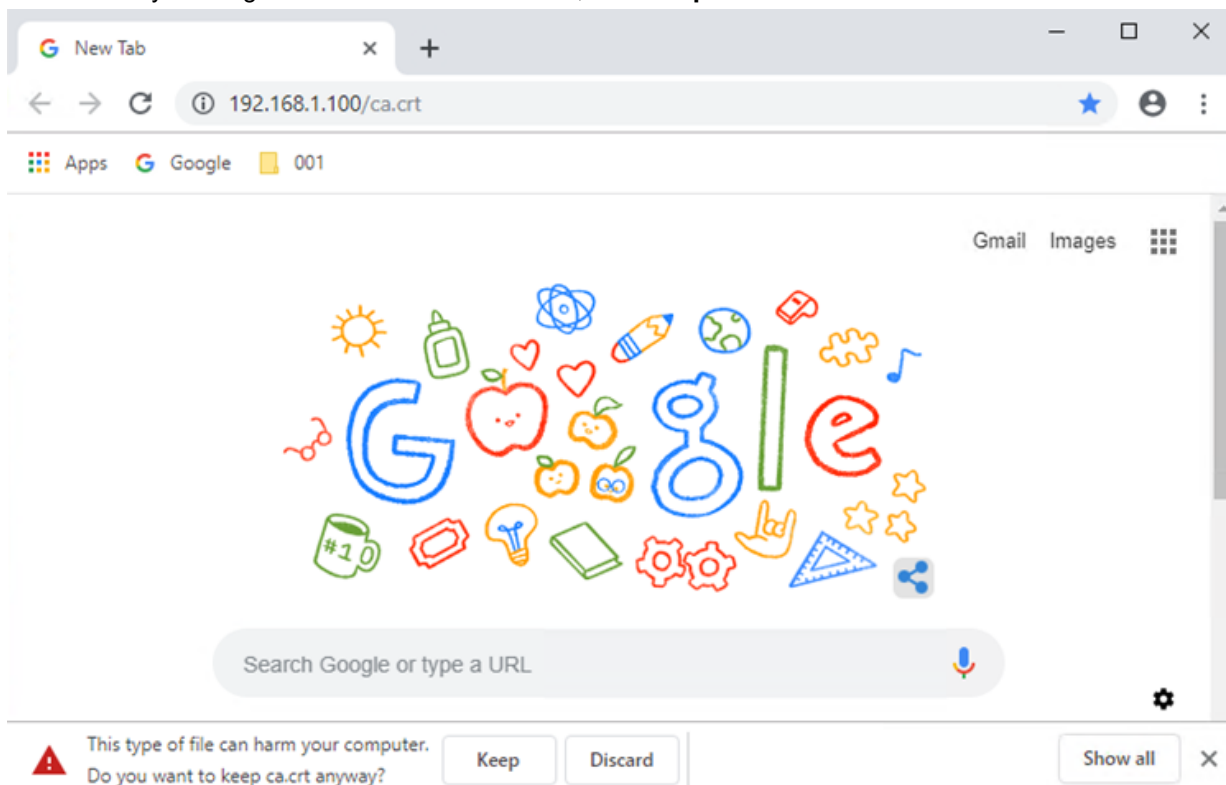
I'm Feeling Lucky

Using IP forwarding mode with Google Chrome

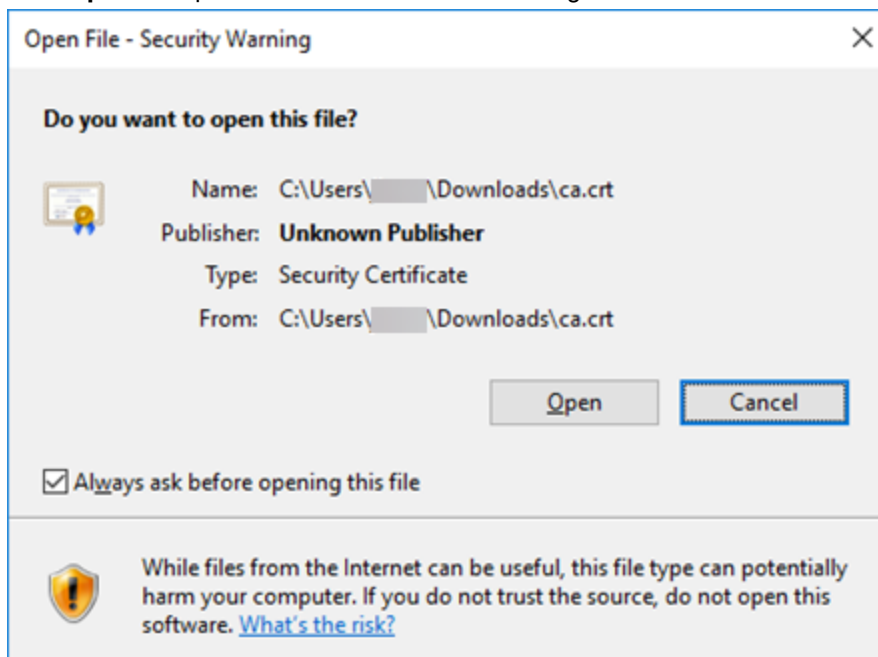
Use this procedure to configure IP forwarding mode with Google Chrome.

Steps

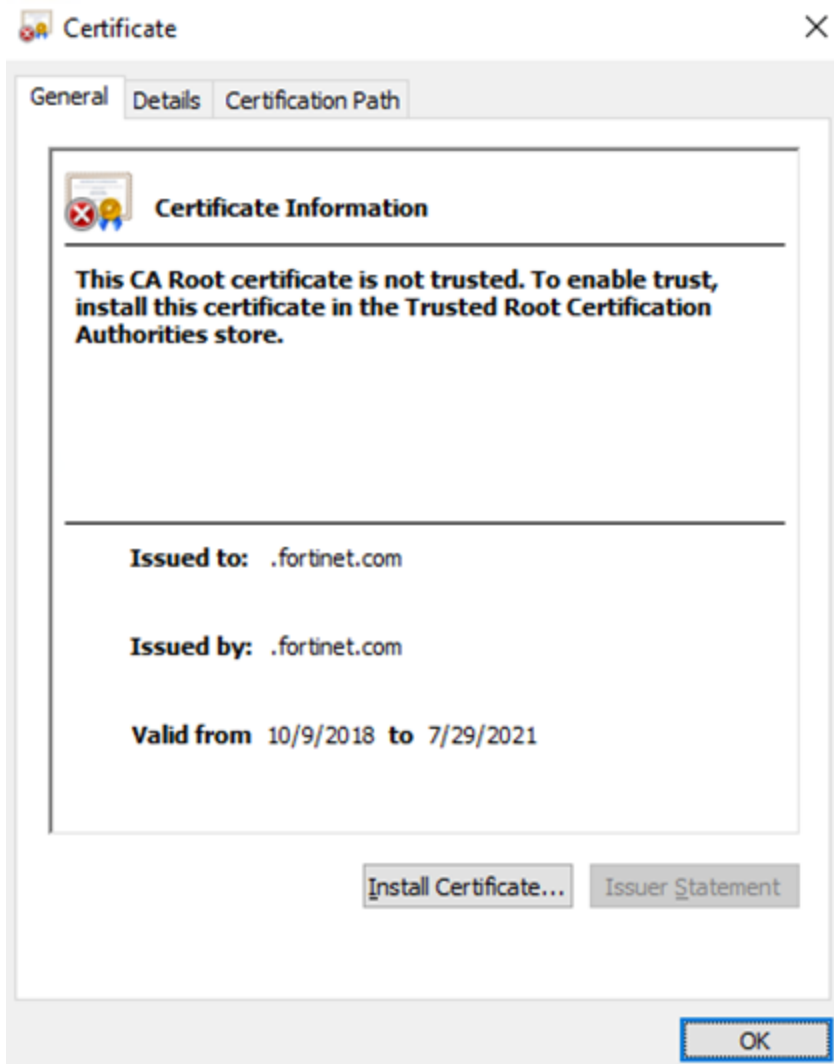
1. To download the Fortisolator certificate (ca.crt) and import it into your Google Chrome browser, follow these steps:
 - a. In the Google Chrome browser address bar, type `http://<internal_IP_address>/ca.crt` (for example, `http://192.168.1.100/ca.crt`).
 - where `<internal_IP_address>` value is the IP address of the Fortisolator internal interface. For example, the IP address of the internal interface that you configured in step 3 of [Fortisolator appliance installation on page 7](#).
 - b. In the security warning at the bottom of the browser, click **Keep** to download the certificate.



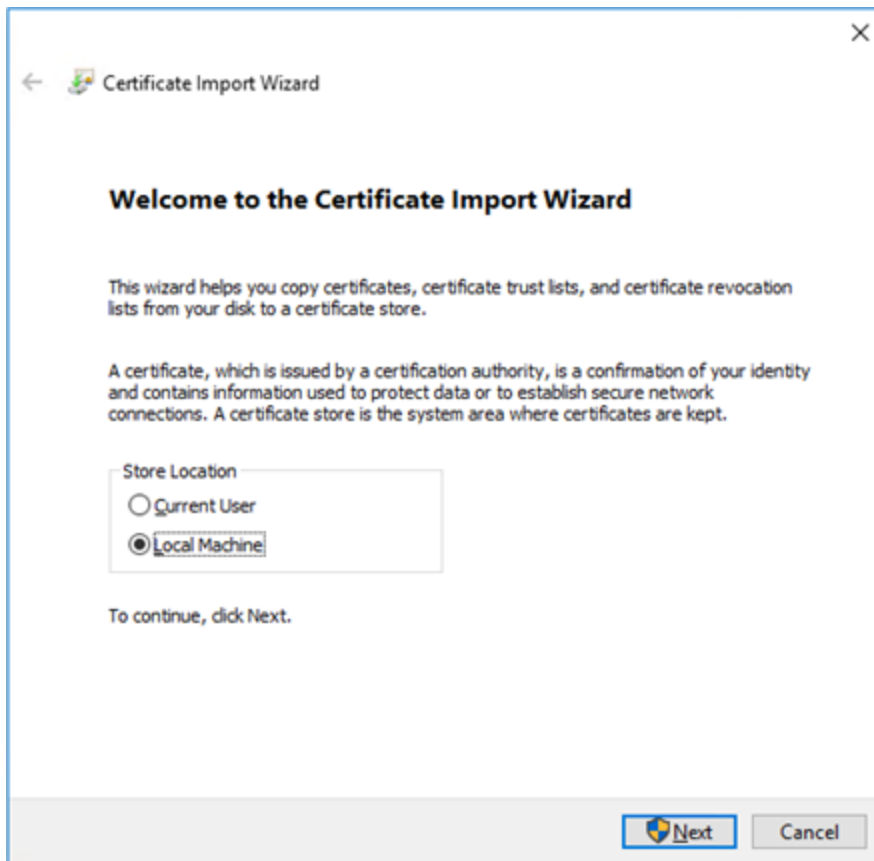
- c. Click **Open** to import the ca.crt certificate into Google Chrome.



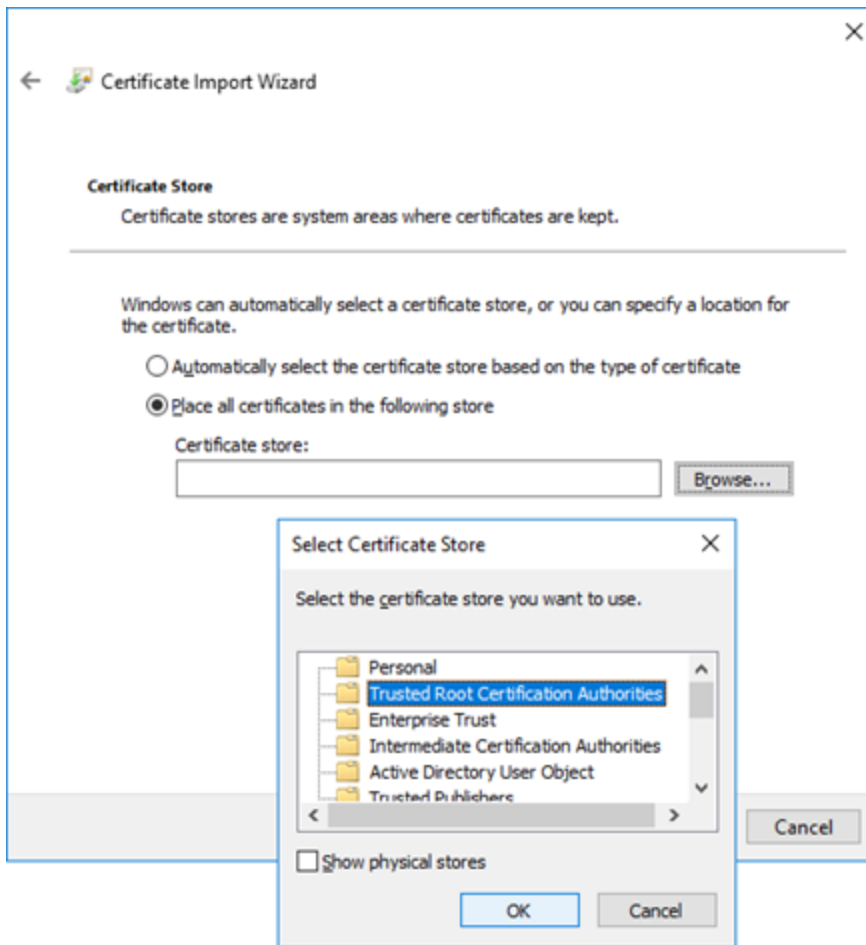
- d. Click **Install Certificate**.



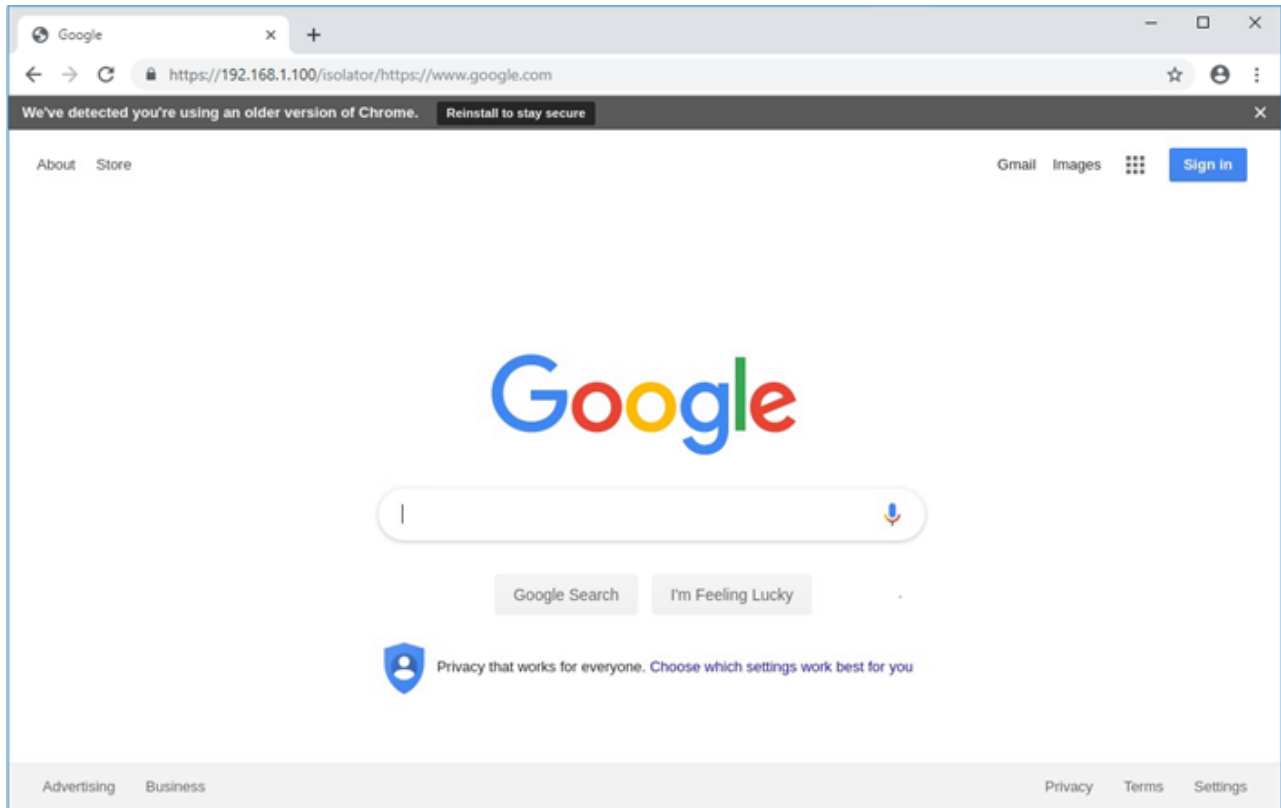
- e. Select **Local Machine**, and click **Next**.



- f. Select **Trusted Root Certification Authorities**, and click **OK**.



2. In the Google Chrome browser address bar, type `https://<internal_IP_address>/isolator/https://www.google.com` (for example, `https://192.168.1.100/isolator/https://www.google.com`).
- where `<internal_IP_address>` value is the IP address of the Fortisolator internal interface



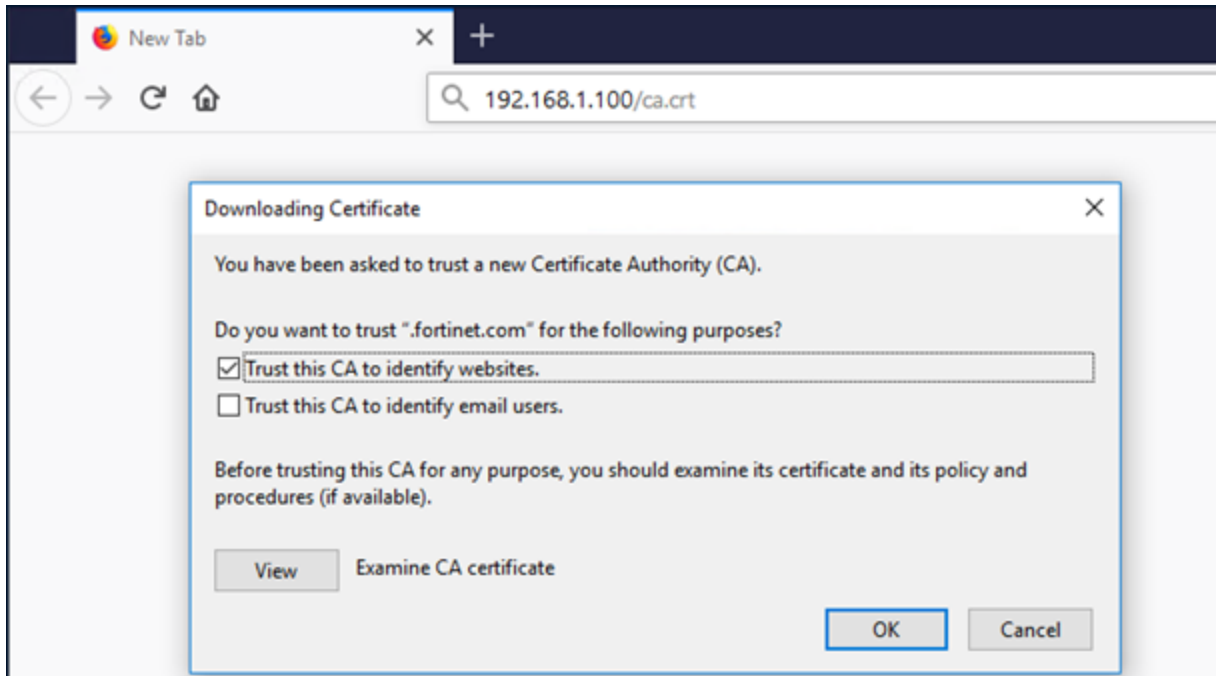
Proxy mode

Using proxy mode with Mozilla Firefox

Use this procedure to configure proxy mode with Mozilla Firefox.

Steps

1. To download the Fortisolator certificate (ca.crt) and import it into the Mozilla Firefox browser, follow these steps:
 - a. In the Mozilla Firefox browser address bar, type `http://<internal_IP_address>/ca.crt` (for example, `http://192.168.1.100/ca.crt`).
 - where `<internal_IP_address>` is the IP address of the Fortisolator internal interface. For example, the IP address of the internal interface that you configured in step 3 of [Fortisolator appliance installation on page 7](#).
 - b. In the **Downloading Certificate** window, select the **Trust this CA to identify websites** checkbox.
 - c. Click **OK**



2. Open the Mozilla Firefox browser.
3. In the menu, click **Options**.
4. Click **General**.
5. In the **Network Settings** section, click **Settings**.
6. In the **Connection Settings** window, select **Manual proxy configuration**, and enter the following settings (values shown here are examples):
 - **HTTP Proxy**: 192.168.1.100, **Port**: 8888
 - **SSL Proxy**: 192.168.1.100, **Port**: 8888
 - **No Proxy for**: "localhost, 127.0.0.1,<internal_IP_address>/24", where <internal_IP_address> is the IP address of the Fortisolator internal interface. For example , the IP address of the internal interface that you configured in step 3 of [Fortisolator appliance installation on page 7](#).
7. Click **OK**.

Connection Settings

Configure Proxy Access to the Internet

☐ No proxy

☐ Auto-detect proxy settings for this network

☐ Use system proxy settings

☒ Manual proxy configuration

HTTP Proxy

192.168.1.100

Port

8888

☐ Use this proxy server for all protocols

SSL Proxy

192.168.1.100

Port

8888

FTP Proxy

Port

0

SOCKS Host

Port

0

☐ SOCKS v4

☒ SOCKS v5

☐ Automatic proxy configuration URL

Reload

No proxy for

localhost, 127.0.0.1, 192.168.1.0/24

Example: .mozilla.org, .net.nz, 192.168.1.0/24

☐ Do not prompt for authentication if password is saved

☐ Proxy DNS when using SOCKS v5

☐ Enable DNS over HTTPS

☒ Use default (<https://mozilla.cloudflare-dns.com/dns-query>)

☐ Custom

OK

Cancel

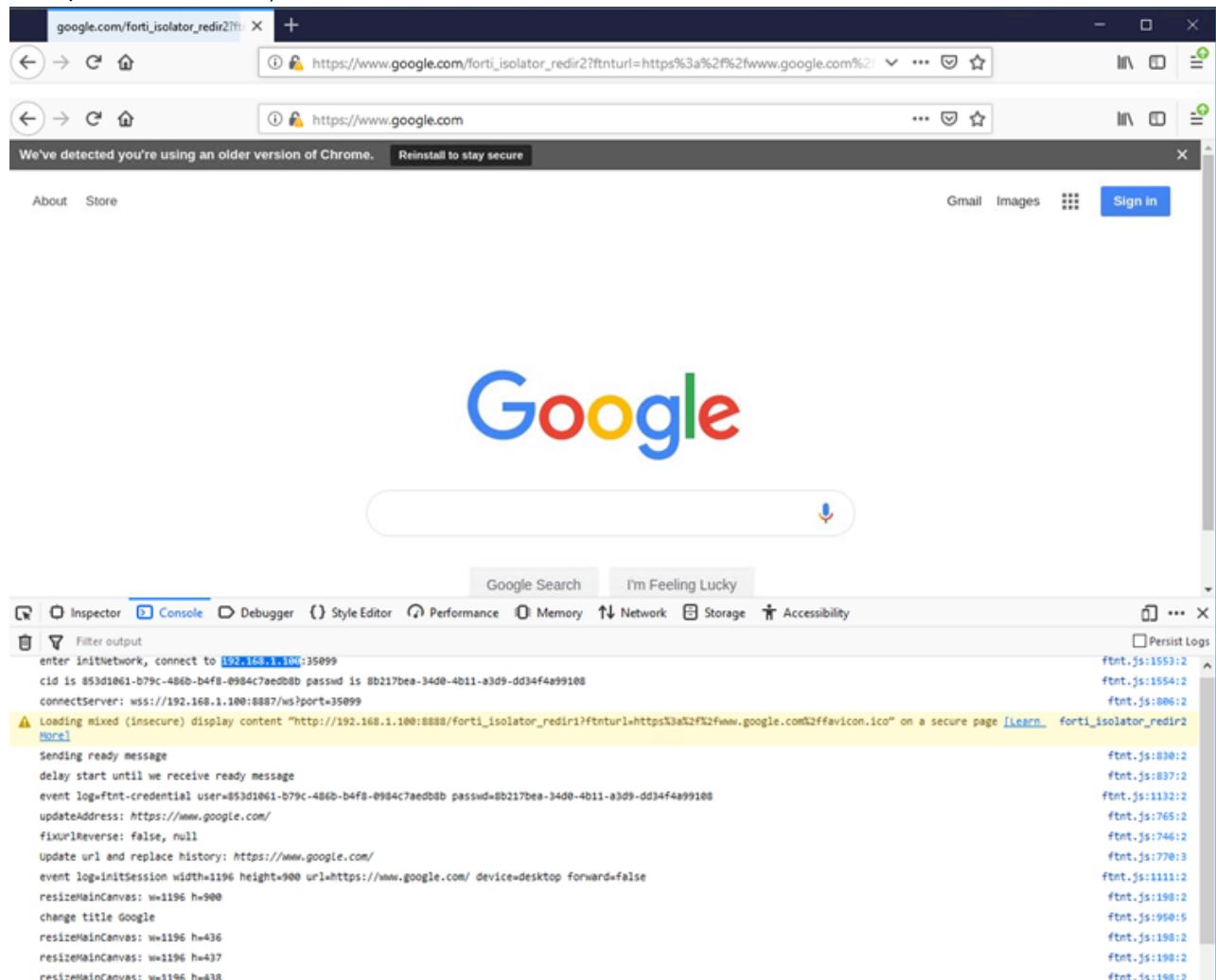
Help

Verifying Fortisolator proxy mode with Mozilla Firefox

Use this procedure to verify that Fortisolator proxy mode is working correctly with Mozilla Firefox.

Steps

1. In the Mozilla Firefox browser, type: `https://www.google.com`.
The URL redirects the browser to `forti_isolator` for a short period of time. For example, `https://www.google.com/forti_isolator_redir2?ftnturl=https%3a%2f%2fwww.google.com%2f&ftntcid=5f4084e8-7978-4c89-97c5-31ef3640600c&ftntpasswd=35026d03-9a1c-42e9-959e-fca18d67e4c0`.
The page should load successfully with the URL displayed as you typed it (`https://www.google.com`).
2. Check the browser console to make sure that it is connecting to the internal IP address of Fortisolator (for example, `192.168.1.100`).



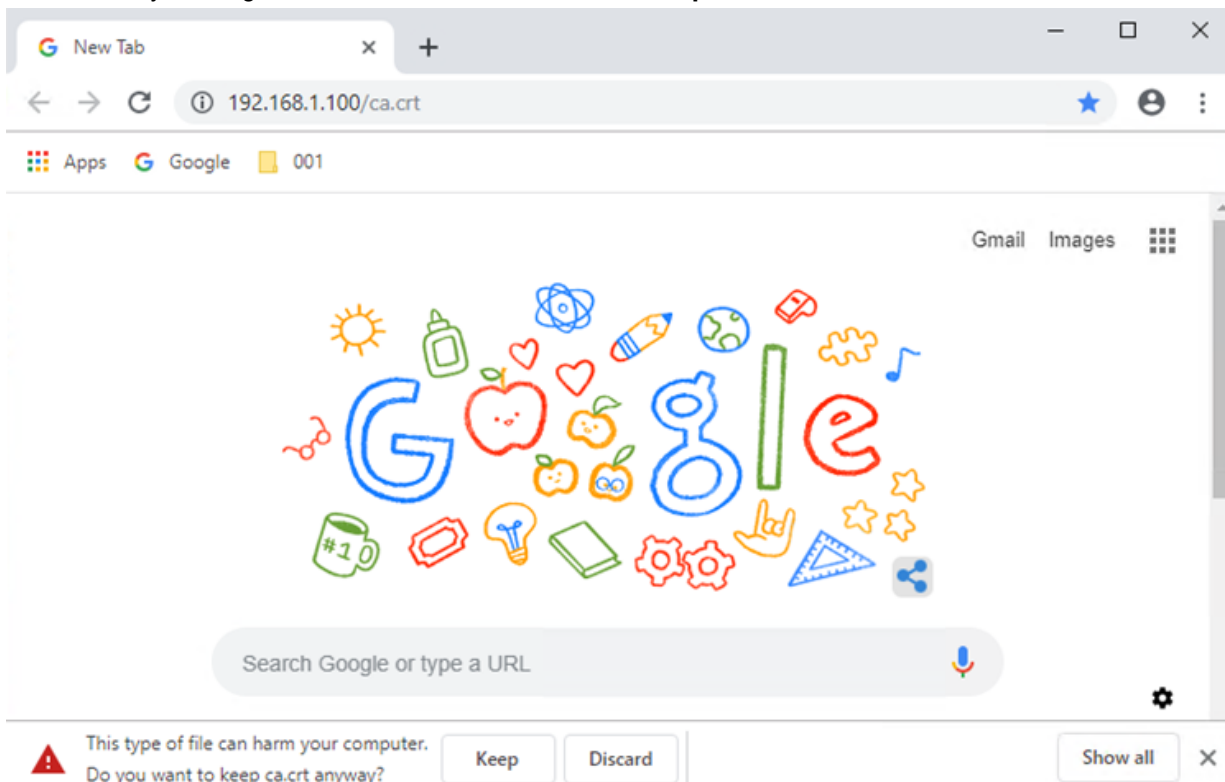
Using proxy mode with Google Chrome

Use this procedure to configure proxy mode with Google Chrome.

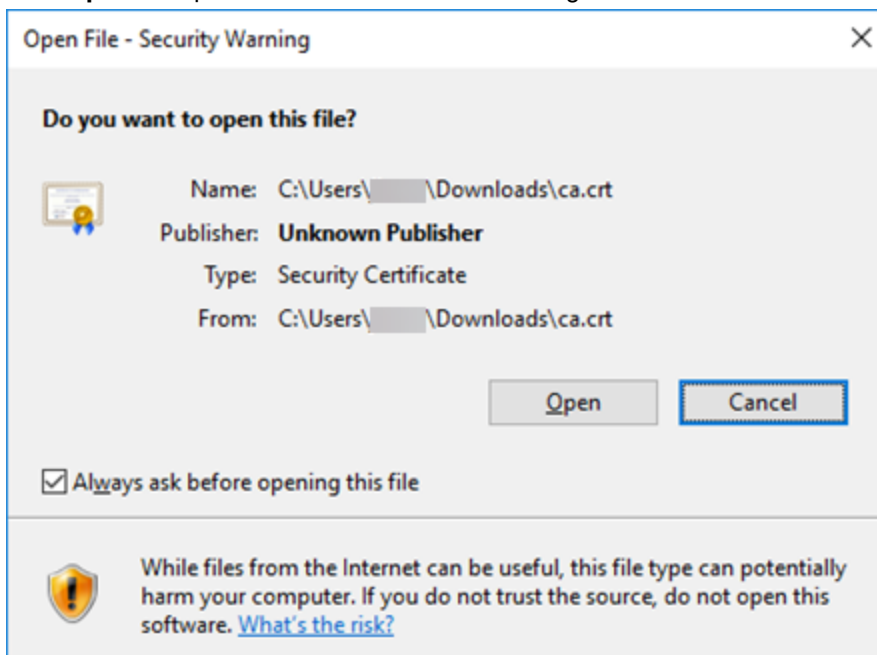
Steps

1. To download the Fortisolator certificate (`ca.crt`) and import it into your Google Chrome browser, follow these steps:

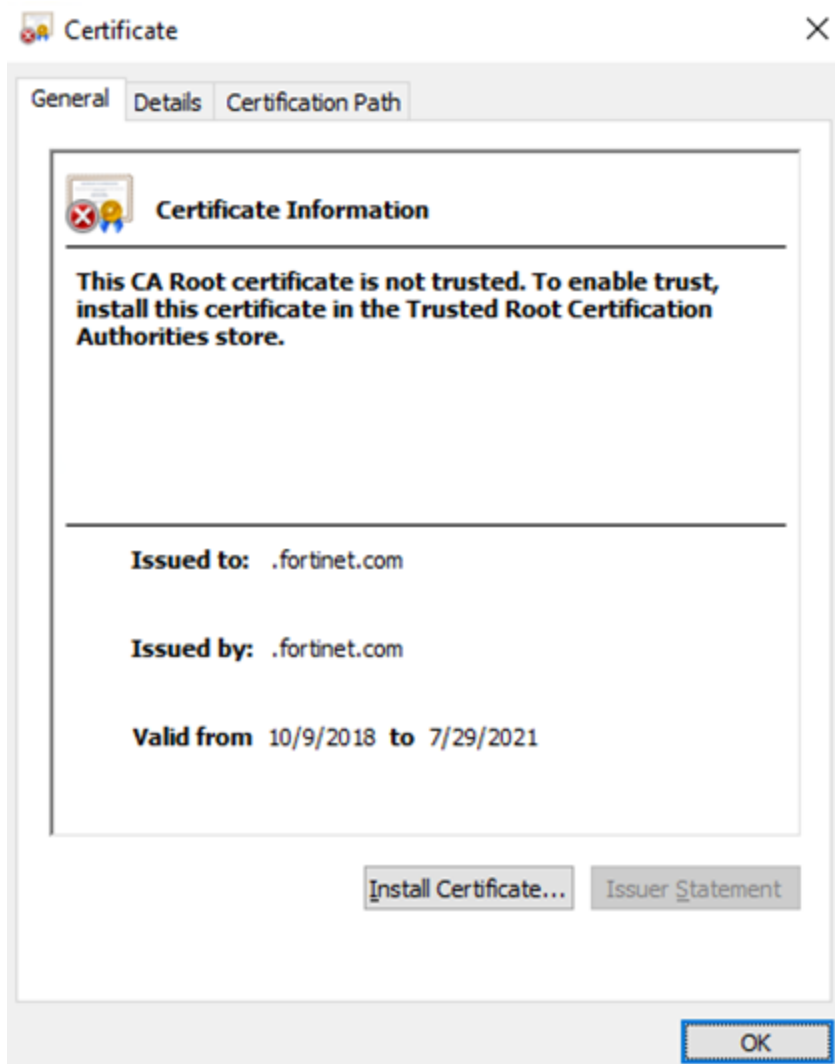
- a. In the Google Chrome browser address bar, type `http://<internal_IP_address>/ca.crt` (for example, `http://192.168.1.100/ca.crt`).
 - where `<internal_IP_address>` value is the IP address of the Fortisolator internal interface. For example, the IP address of the internal interface that you configured in step 3 of [Fortisolator appliance installation on page 7](#).
- b. In the security warning at the bottom of the browser, click **Keep** to download the certificate.



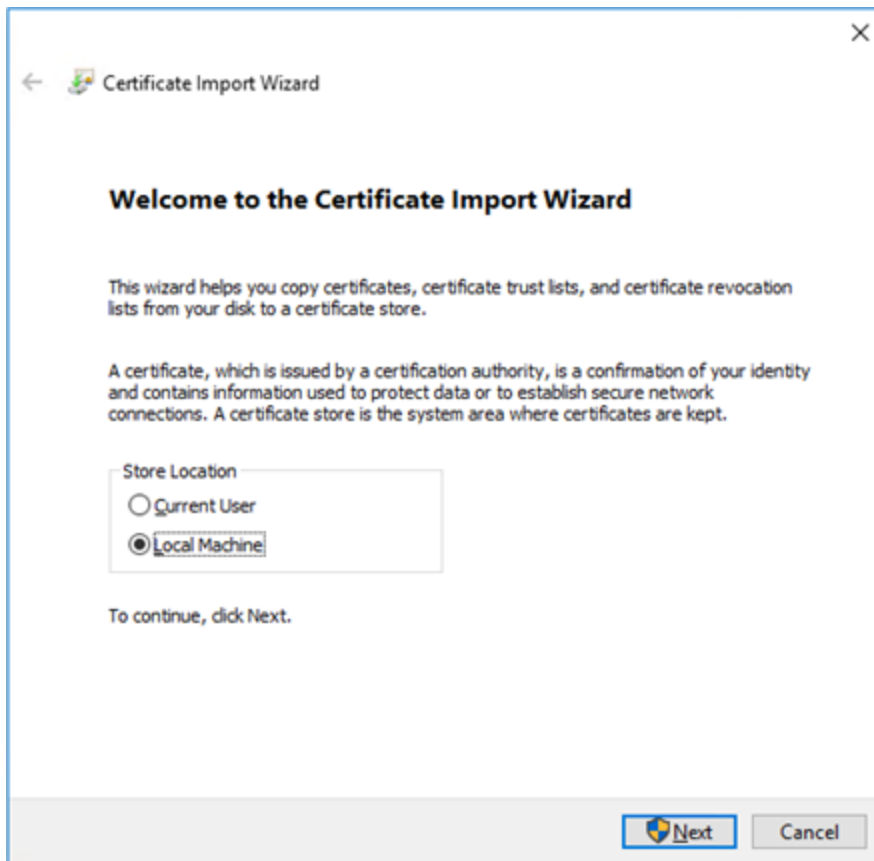
- c. Click **Open** to import the ca.crt certificate into Google Chrome.



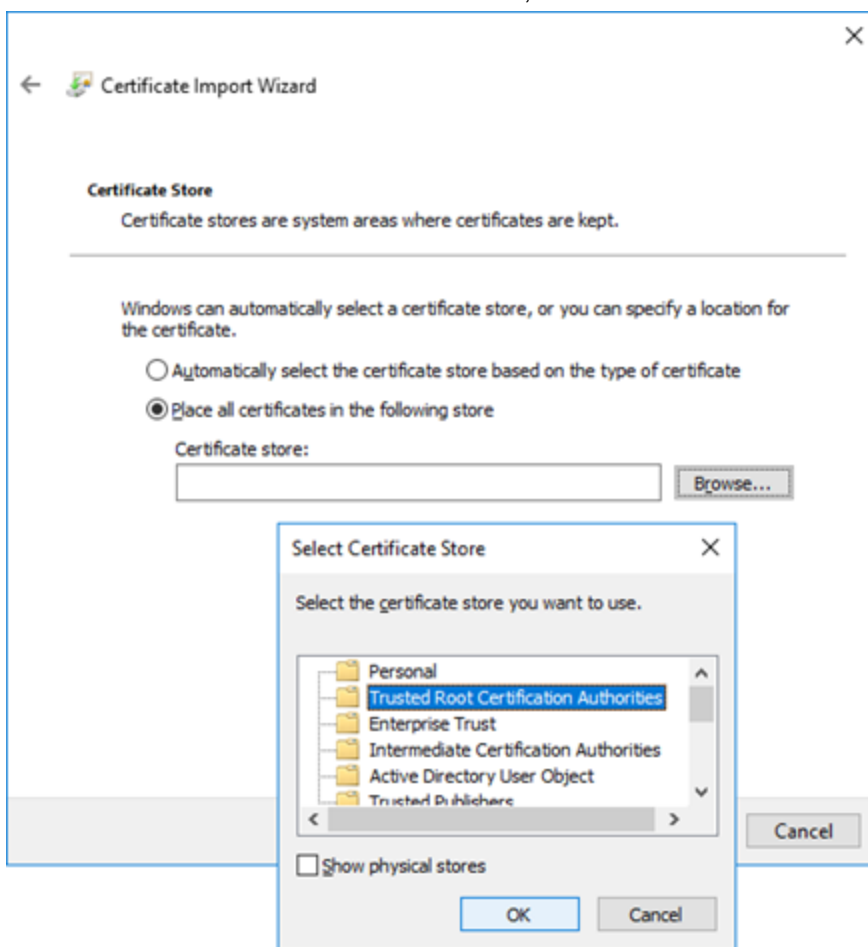
- d. Click **Install Certificate**.



- e. Select **Local Machine**, and click **Next**.

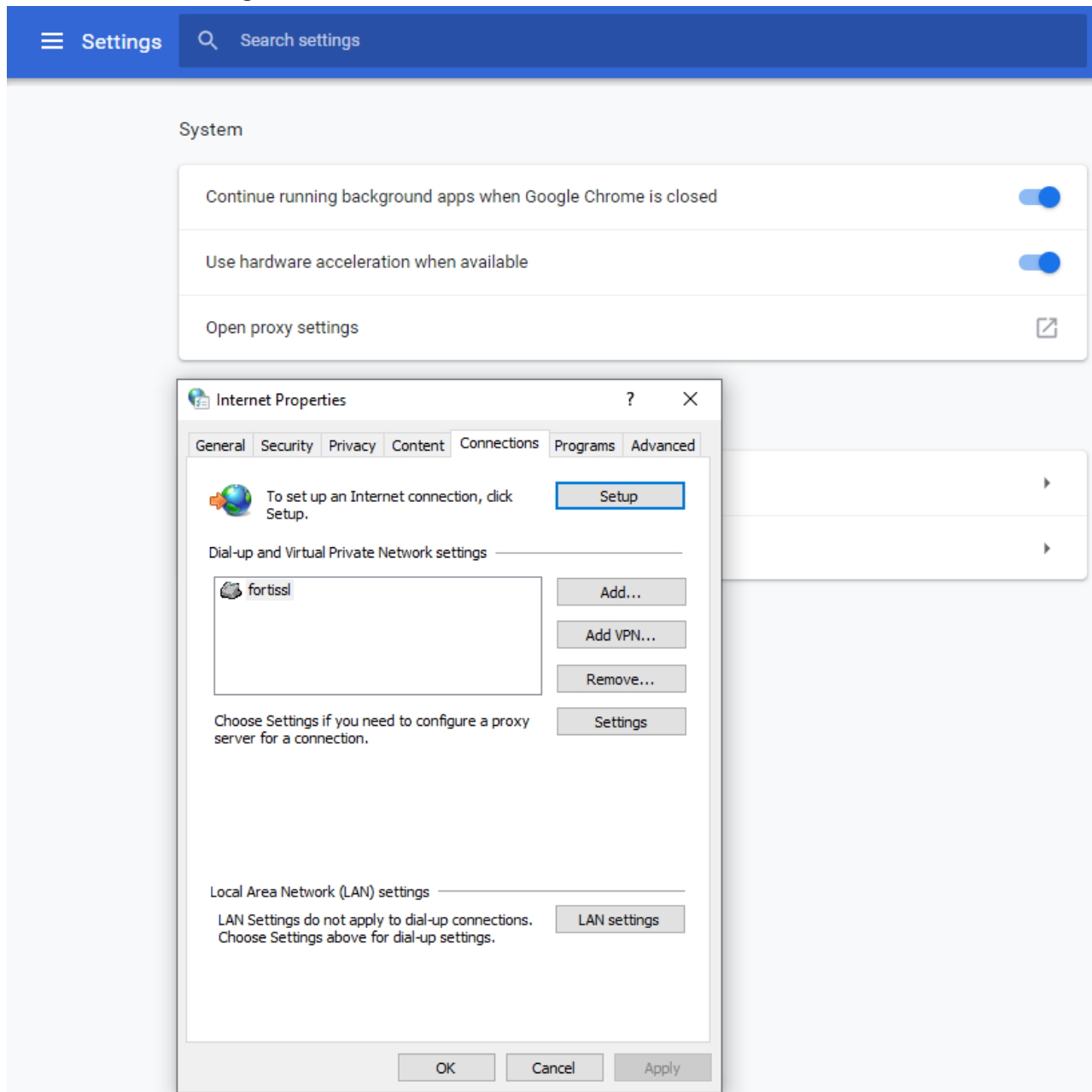


- f. Select **Trusted Root Certificate Authorities**, and click **OK**.

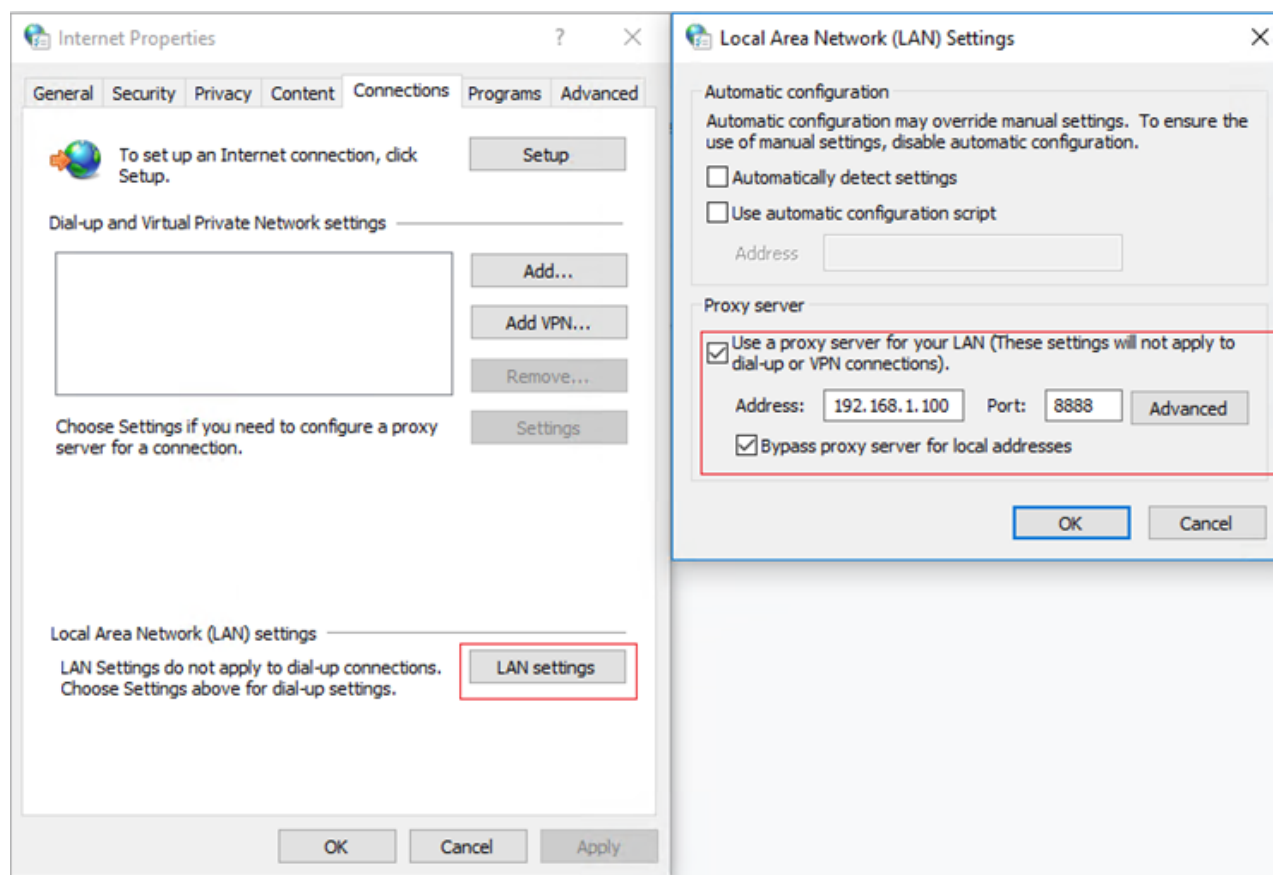


2. Open the Google Chrome browser.

3. In the menu, click **Settings**.

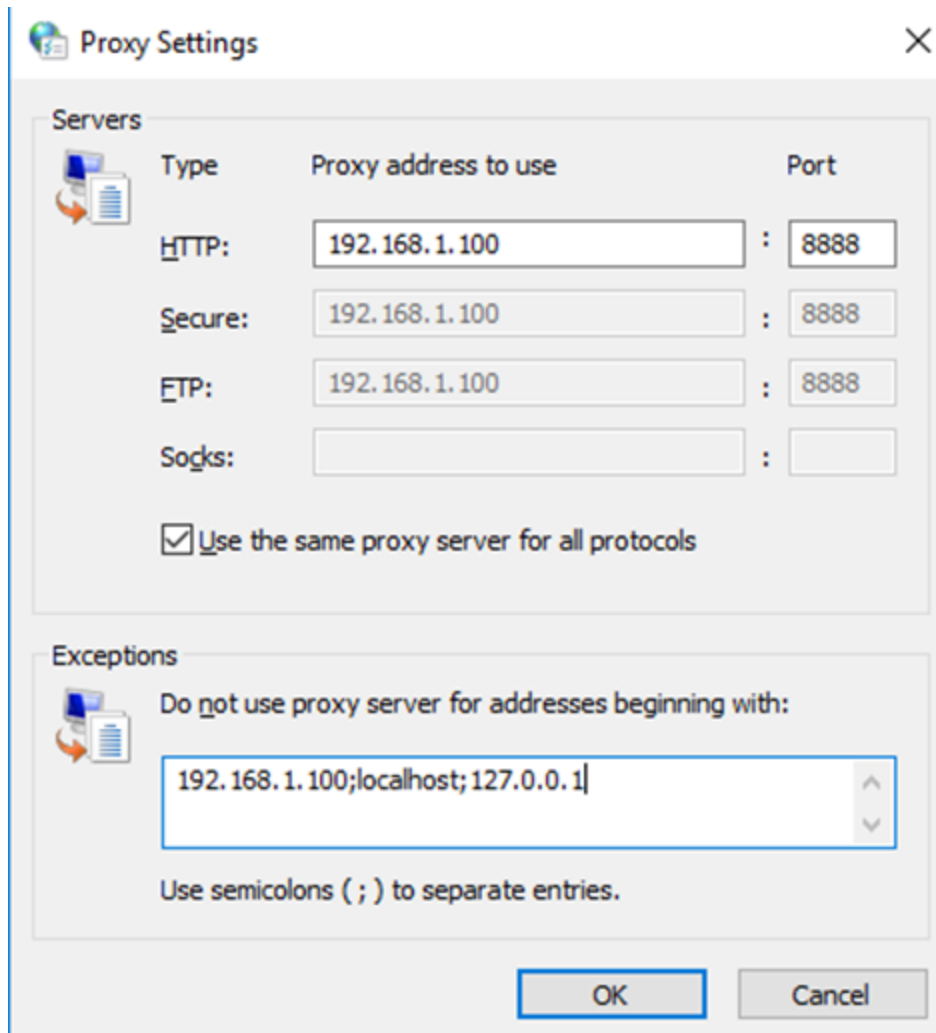


4. Expand **Advanced**.
5. In the **System** section, click **Open proxy settings**.
6. In the **Internet Properties** window, click the **Connections** tab.
7. Click **LAN settings**.
8. In the **Proxy server** section, select **Use a proxy server for your LAN**, and enter the following setting (values shown here are examples):
 - **Address:** 192.168.1.100, **Port:** 8888



9. Click **Advanced**.

10. In the **Proxy Settings** window, in the **Exceptions** section, type **192.168.1.100;localhost;127.0.0.1** (values used here are examples).



11. Click **OK** to accept the settings in all windows.

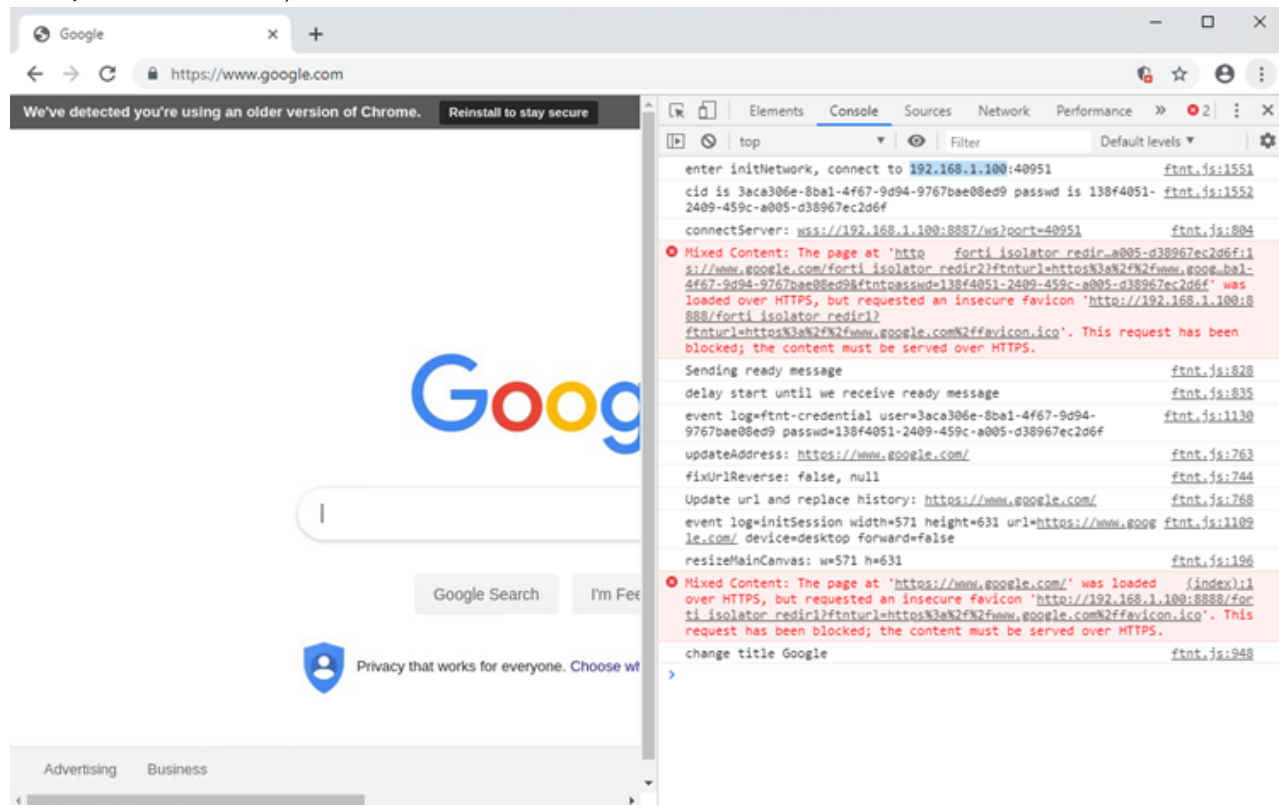
Verifying Fortisolator proxy mode with Google Chrome

Use this procedure to verify that Fortisolator proxy mode is working correctly with Google Chrome.

Steps

1. In the Google Chrome browser, type: `https://www.google.com`.
The URL redirects the browser to `forti_isolator` for a short period of time. For example, `https://www.google.com/forti_isolator_redir2?ftnturl=https%3a%2f%2fwww.google.com%2f&ftntcid=3aca306e-8ba1-4f67-9d94-9767bae08ed9&ftntpasswd=138f4051-2409-459c-a005-d38967ec2d6f`.
The page should load successfully with the URL displayed as you typed it (`https://www.google.com`).
2. Check the browser console to make sure that it is connecting to the internal IP address of Fortisolator (for

example, 192.168.1.100).



PAC file mode

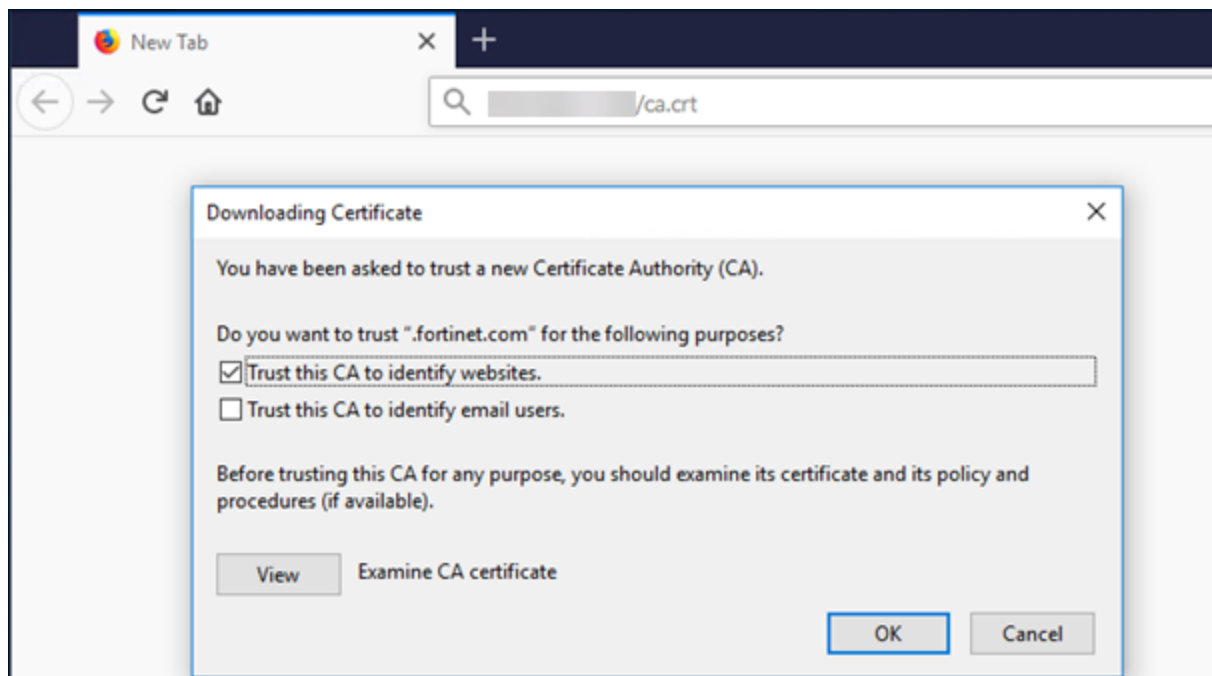
PAC file mode with Mozilla Firefox

Importing the Fortisolator certificate into the Mozilla Firefox browser

Use this procedure to import the Fortisolator certificate into the Mozilla Firefox browser.

Steps

1. To download the Fortisolator certificate (ca.crt) and import it into the Mozilla Firefox browser, follow these steps:
 - a. In the Mozilla Firefox browser address bar, type `http://<internal_IP_address>/ca.crt`.
 - where `<internal_IP_address>` is the IP address of the Fortisolator internal interface. For example, the IP address of the internal interface that you configured in step 3 of [Installing Fortisolator 1000F on page 1](#).
 - b. In the **Downloading Certificate** window, select the **Trust this CA to identify websites** checkbox.
 - c. Click **OK**

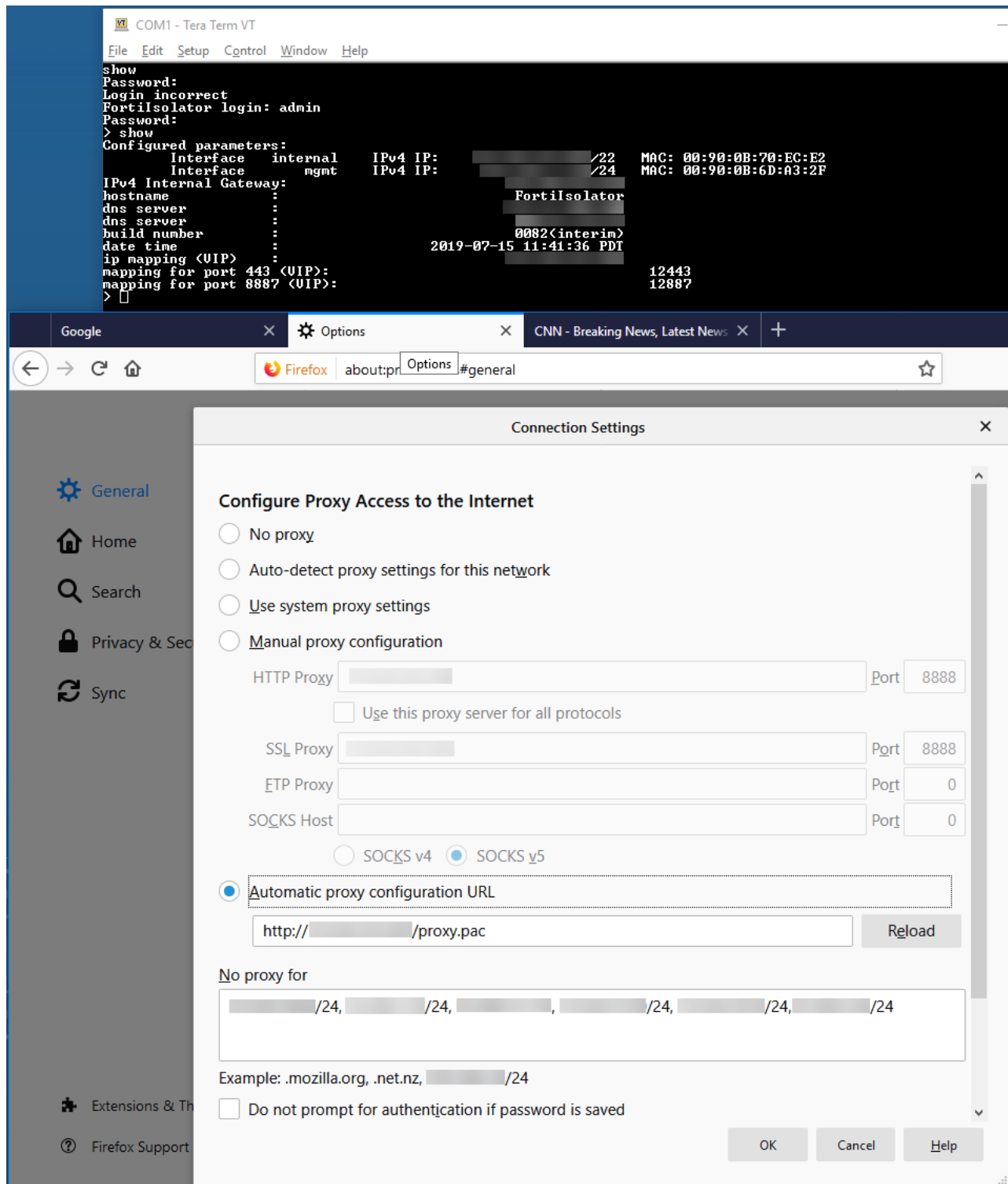


Configuring PAC file mode in Mozilla Firefox

Use this procedure to configure PAC file mode in Mozilla Firefox.

Steps

1. Open the Mozilla Firefox browser.
2. In the menu, click **Options**.
3. Click **General**.
4. In the **Network Settings** section, click **Settings**.
5. In the **Connection Settings** window, select **Automatic proxy configuration URL**, and enter `http://<internal_IP_address>/proxy.pac`.



6. Click **OK**.

Connection Settings

Configure Proxy Access to the Internet

☐ No proxy

☐ Auto-detect proxy settings for this network

☐ Use system proxy settings

☒ Manual proxy configuration

HTTP Proxy Port

☐ Use this proxy server for all protocols

Port

Port

Port

☐ SOCKS v4 ☒ SOCKS v5

☒ Automatic proxy configuration URL

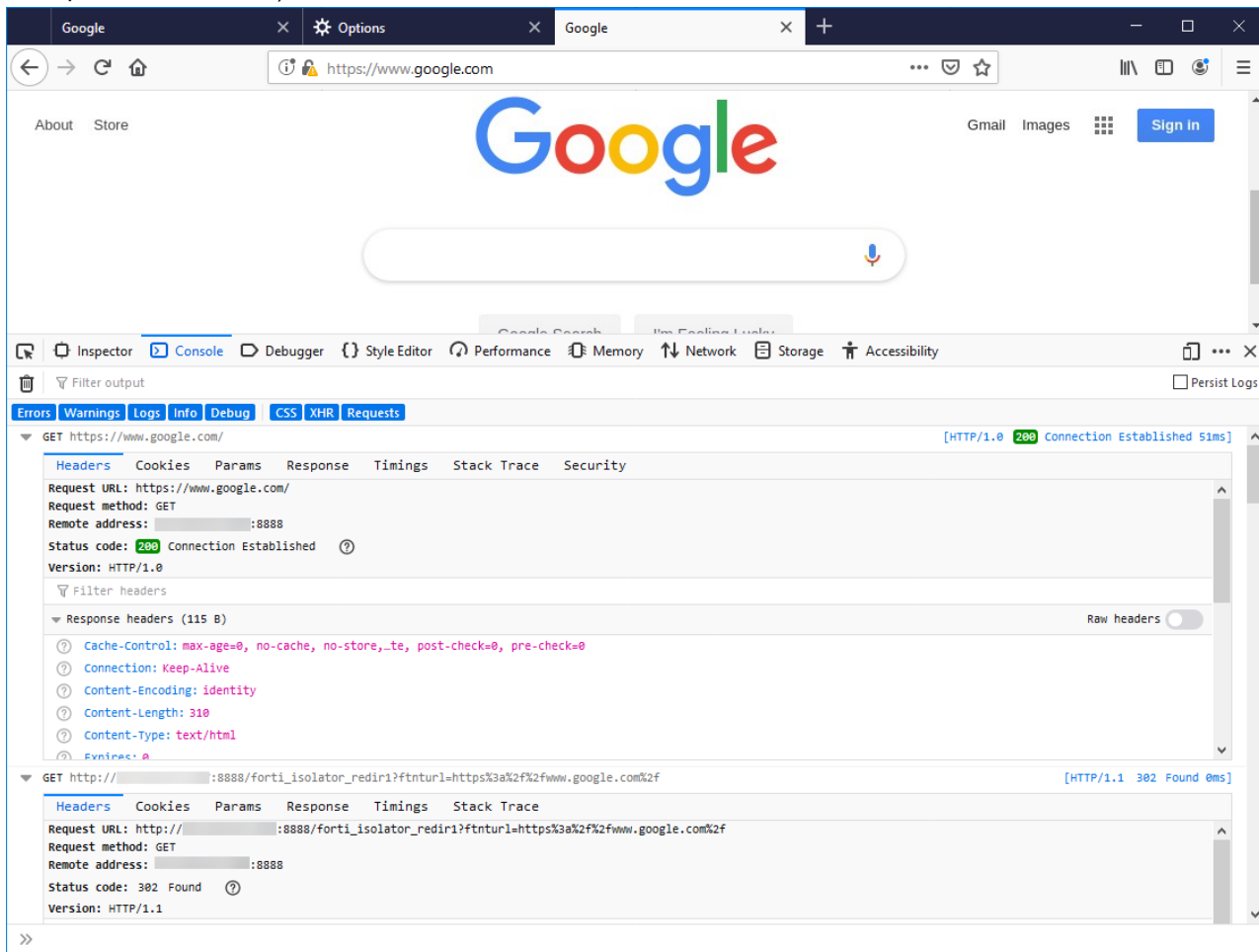
Verifying Fortisolator PAC file mode with Mozilla Firefox

Use this procedure to verify that Fortisolator PAC file mode is working correctly with Mozilla Firefox.

Steps

1. In the Mozilla Firefox browser, type: `https://www.google.com`.
The URL redirects the browser to `forti_isolator` for a short period of time. For example, `https://www.google.com/forti_isolator_redir2?ftnturl=https%3a%2f%2fwww.google.com%2f&ftntcid=853d1061-b79c-486b-b4f8-0984c7aedb8b&ftntpasswd=8b217bea-34d0-4b11-a3d9-dd34f4a99108`.
The page should load successfully with the URL displayed as you typed it (`https://www.google.com`).
2. Check the browser console to make sure that it is connecting to the internal IP address of Fortisolator (for

example, 192.168.1.100).



PAC file mode with Google Chrome

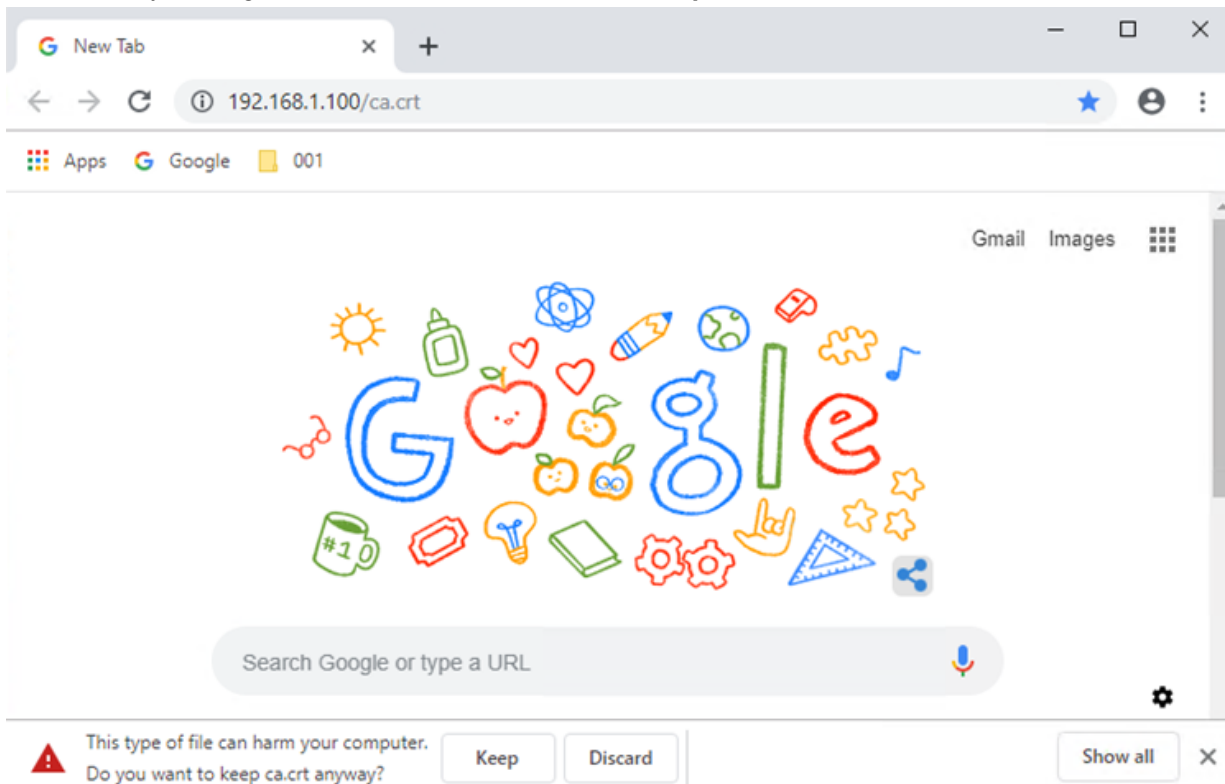
Importing the Fortisolator certificate into the Google Chrome browser

Use this procedure to import the Fortisolator certificate into the Google Chrome browser.

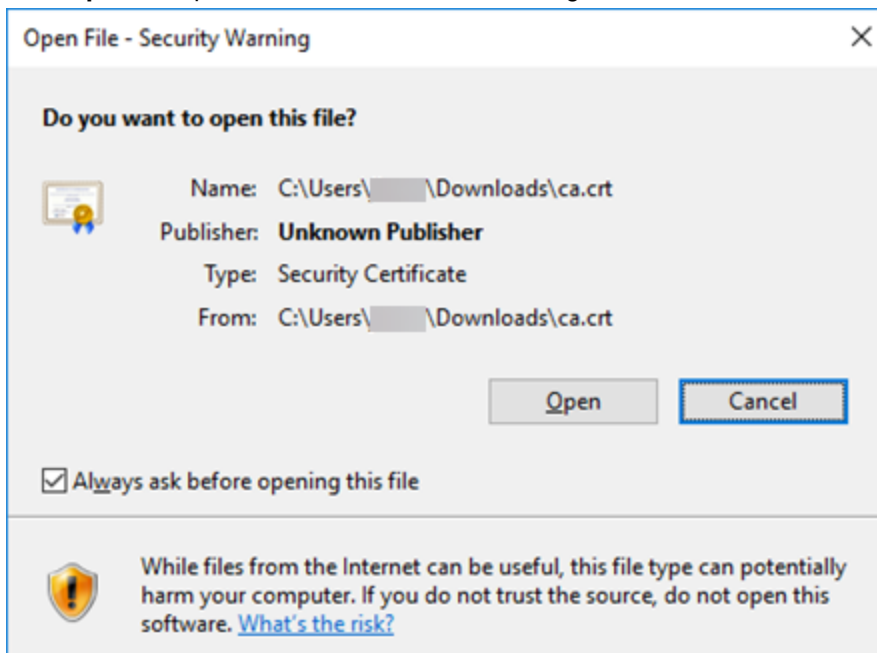
Steps

1. To download the Fortisolator certificate (ca.crt) and import it into the Google Chrome browser, follow these steps:
 - a. In the Google Chrome browser address bar, type `http://<internal_IP_address>/ca.crt` (for example, `http://192.168.1.100/ca.crt`).
 - where `<internal_IP_address>` value is the IP address of the Fortisolator internal interface. For example, the IP address of the internal interface that you configured in step 3 of [Fortisolator appliance installation on page 7](#).

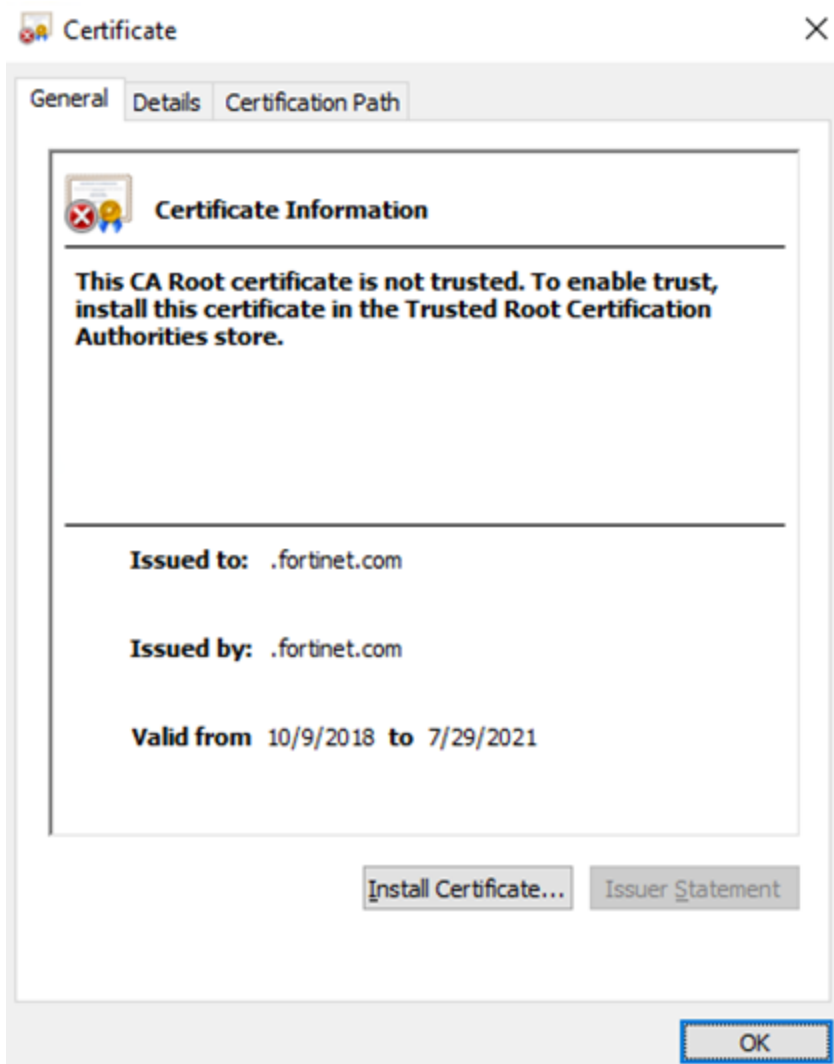
- b. In the security warning at the bottom of the browser, click **Keep** to download the certificate.



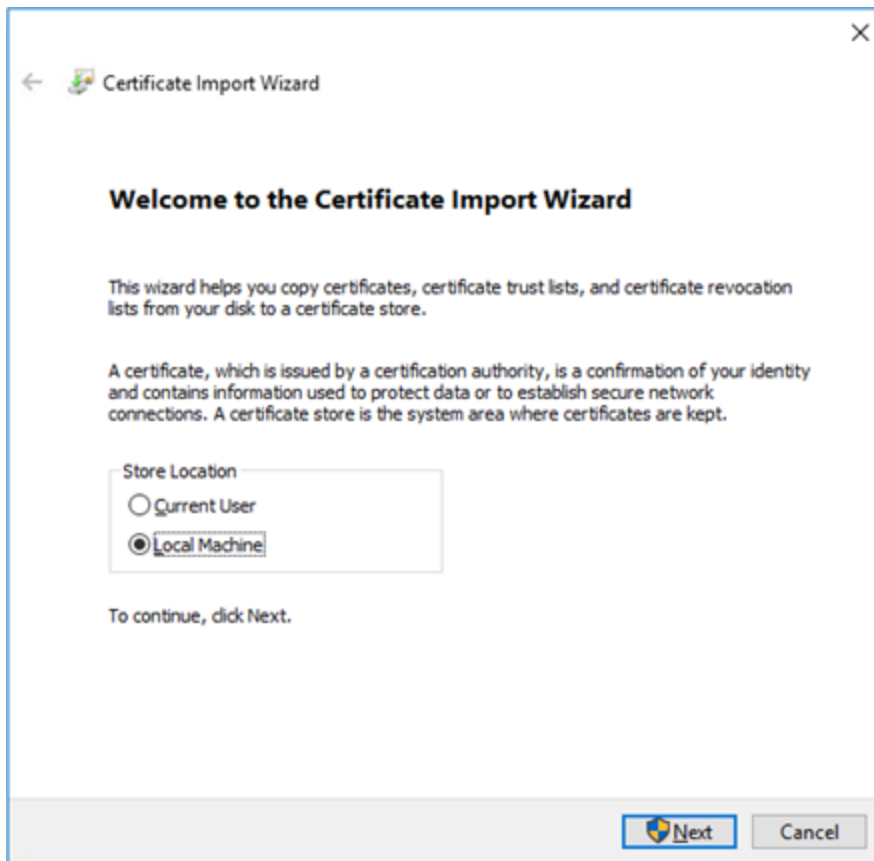
- c. Click **Open** to import the ca.crt certificate into Google Chrome.



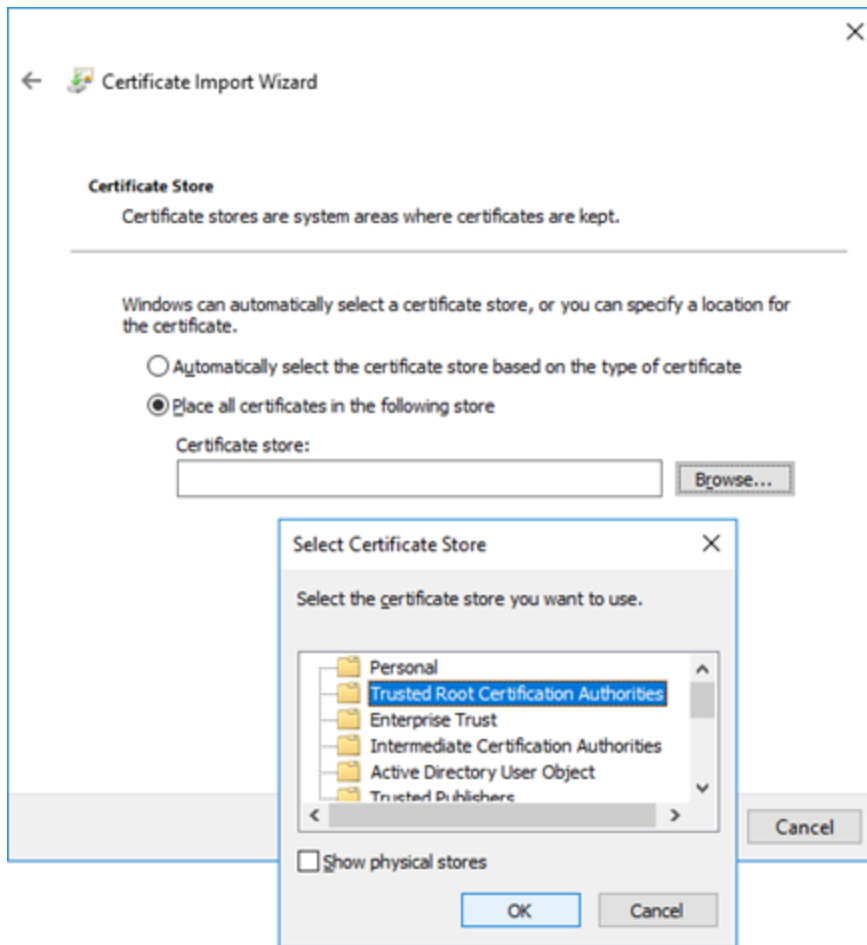
- d. Click **Install Certificate**.



- e. Select **Local Machine**, and click **Next**.



- f. Select **Trusted Root Certification Authorities**, and click **OK**.



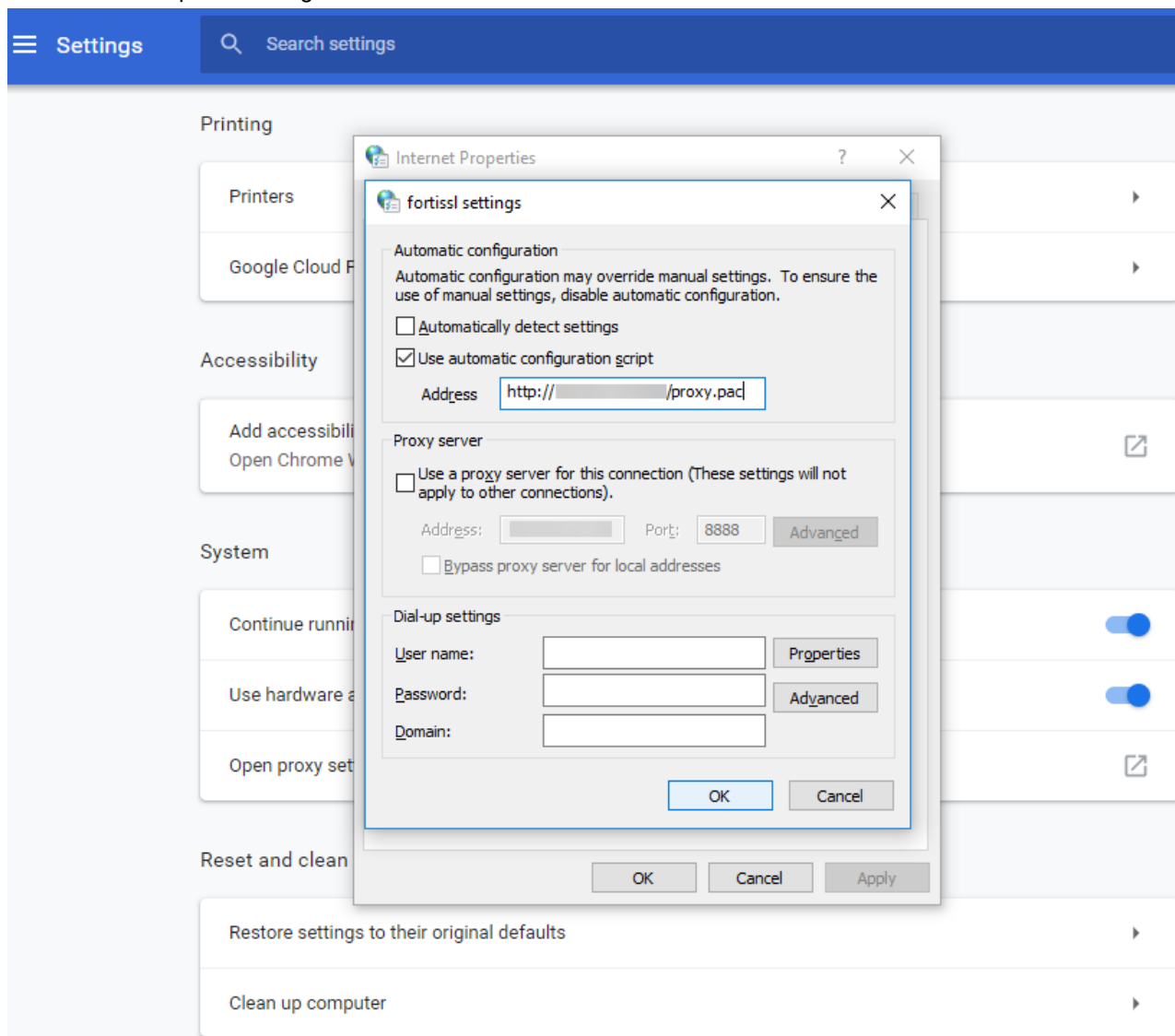
Configuring PAC file mode in Google Chrome

Use this procedure to configure PAC file mode in Google Chrome.

Steps

1. Open the Google Chrome browser.
2. In the menu, click **Settings**.
3. Expand **Advanced**.
4. In the **System** section, click **Open proxy settings**.
5. In the **Internet Properties** window, click the **Connections** tab.
6. Click **LAN settings**.
7. In the **Automatic configuration** section, select **Use automatic configuration script**, and enter `http://<internal_IP_address>/proxy.pac` in the **Address** field.

- Click **OK** to accept the settings in all windows.



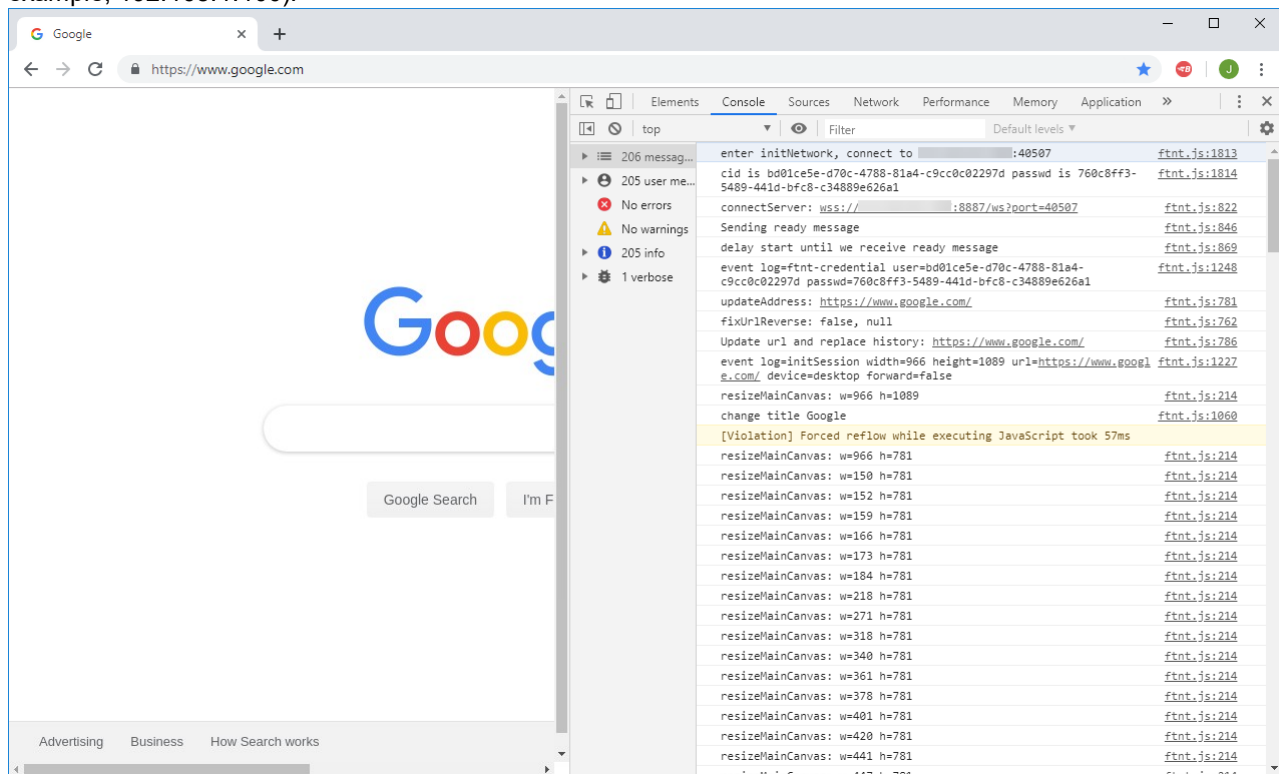
Verifying Fortisolator PAC file mode with Google Chrome

Use this procedure to verify that Fortisolator proxy mode is working correctly with Google Chrome.

Steps

- In the Google Chrome browser, type: `https://www.google.com`.
The URL redirects the browser to `forti_isolator` for a short period of time. For example, `https://www.google.com/forti_isolator_redir2?ftnturl=https%3a%2f%2fwww.google.com%2f&ftntcid=3aca306e-8ba1-4f67-9d94-9767bae08ed9&ftntpasswd=138f4051-2409-459c-a005-d38967ec2d6f`.
The page should load successfully with the URL displayed as you typed it (`https://www.google.com`).

2. Check the browser console to make sure that it is connecting to the internal IP address of Fortisolator (for example, 192.168.1.100).



Copying and pasting text

Use this procedure to copy and paste text in a browser that is running through Fortisolator.

Steps

1. In a browser, select text that you want to copy, and then right-click.
2. Click **Copy**.
3. Navigate to the location where you want to paste the text, and then right-click.
4. Click **Paste**.

Diagnostics

Diagnostic tools

Tool	Definition
ping	Test network connectivity to another network host.
hardware-info	Display general hardware status information.
diagnose-nic	Display general network interface setting.



FORTINET®



Copyright© 2019 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.